Handbuch

Security Operation Center

Version 2.0



•O• SECUREPOINT

Inhalt

Vorwort

Das Security Operation Center (SOC) stellt die neue Verwaltungssoftware für Securepoint Appliances dar. Das Konzept wurde an das Administrations Webinterface der Securepoint Firewall Version 10 angepasst.
Über das Operation Center können übergeordnete Administrationsaufgaben wie Monitoring und Backup erledigt werden. Wie vom Securepoint Security Manager gewohnt, bleibt die Möglichkeit der direkten SSH-Verbindung zu einzelnen Firewalls bestehen und bietet Ihnen die vom Administrations-Webinterface gewohnten Einstellungsmöglichkeiten. Lediglich einige Ansichten des Webinterface sind nicht verfügbar, da die Verbindung per SSH hergestellt wird und nicht wie üblich per HTTPS.
Das Security Operation Center wird lokal auf einem Rechner installiert. Mit dem Operation Center werden mehrere Dienste und Datenbanken installiert, die dem Programm Daten zur Verfügung stellen und verwalten. Alle Dienste können lokal auf einem Computer installiert sein oder zentral auf einem Server gehalten werden, um mehreren Benutzer den Zugriff zu ermöglichen oder von verschiedenen Orten und auch extern auf die Daten zugreifen zu können.
Über den Dienst ***Securepoint Data Provider*** greift das Operation Center auf eine Datenbank zu, in welcher Daten des SOC hinterlegt sind.
Der Dienst ***Securepoint Backup*** speichert Sicherungen der verwalteten Appliances ab.
Der Dienst ***Securepoint Monitor*** ruft Monitoring Daten von den verwalteten Appliances ab und stellt diese dem Operation Center zur Verfügung.
Eingestellte Aufgaben werden vom Dienst ***Securepoint Task*** gespeichert und ausgeführt.
Der Dienst ***Securepoint Logserver Service*** ruft Protokolldaten von den beobachteten Appliances ab, schreib diese in eine Datenbank und stellt sie dem Log Center Client des Operation Centers zur Verfügung.

Das Operation Center bietet Ihnen in der linken Leiste die sieben Bereiche ***Monitoring Center***, ***Extras***, ***Operation Center***, ***Link Center***, ***Service Center***, ***Log Center*** und ***UMT/VPN Gateways Center***. Im rechten Teil des Programmfensters werden aktuelle Last- daten der verwalteten Gateways oder die Administrationsoberfläche angezeigt.
Wenn Sie z. B. direkt an einem Gateway angemeldet sind, wird in dem rechten Fenster das Administrations-Webinterface des jeweiligen Gateway angezeigt. Es können höchstens zu vier Gateways direkte Verbindungen aufgebaut werden.

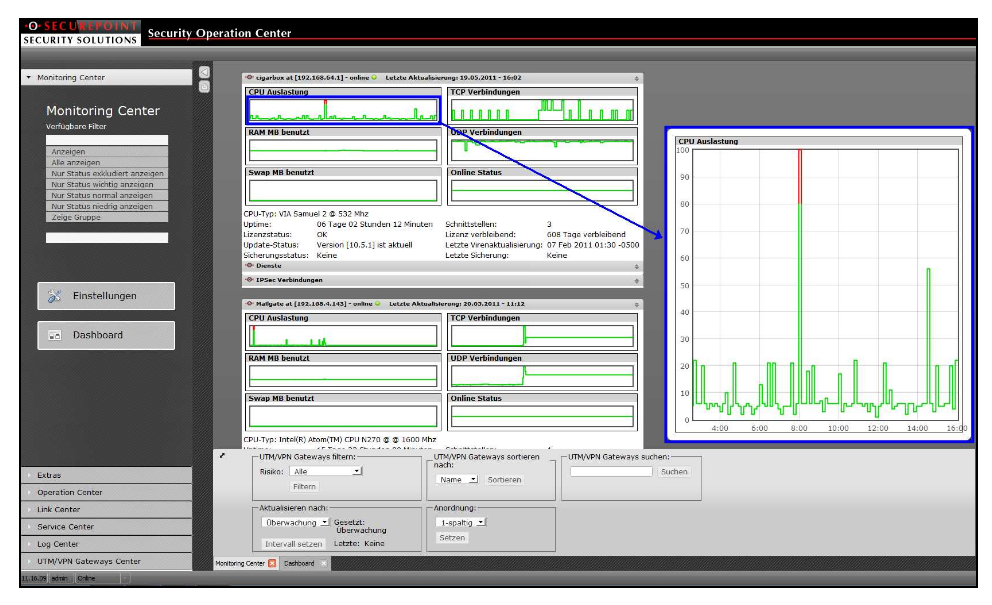


Abb. 1 Überwachungsansicht des Operation Centers

Die geöffneten Ansichten und Verbindungen werden in Karteireitern am unteren Bildrand geführt. Es können bis zu neun Registerkarten (Tabs) gleichzeitig geöffnet sein. Die Reihen- folge der Registerkarten kann durch Drag und Drop nach den eigenen Wünschen gestaltet werden.
Sind mehrere Verbindungen zu Gateways geöffnet, werden bei Bearbeitung einer Appliance die Verbindungen zu den anderen Appliances geblockt, da immer nur eine SSH-Verbindung aktiv sein kann.

Folgende Ansichten werden in Tabs geöffnet:

jeweils ein Tab	News, SOC Protokoll, Monitoring, Dashboard, Firewall-Liste
bis zu vier Tabs	Verbindungen zu Appliance
mehrere Tabs	URL-Verbindungen

1 Hinweise zur Installation

Das Security Operation Center ist für Microsoft Windows und Linux Distributionen erhältlich. Die Dienste, welche die Schnittstellen zu verschlüsselten Datenbanken darstellen, können nur auf einem Windows System installiert werden.
Das Softwarepaket für Windows ist eine ausführbare EXE Datei, die einen Installationsassistenten startet. Für Linux Distributionen wird ein komprimiertes TAR-Archiv angeboten.

Das Security Operation Center Installationspaket für Windows setzt sich aus mehreren Komponenten zusammen.
Die Hauptkomponenten sind das Anwendungsprogramm für Clientrechner, das Microsoft C++ Redistributable Package und der Dienst **Datenprovider**. Die zusätzlichen Dienste **Überwachung**, **Sicherung**, **Aufgaben** und **Logserver** sowie der Dienst **Datenprovider** können lokal auf dem Clientrechner als auch auf einem Server zentral installiert werden.

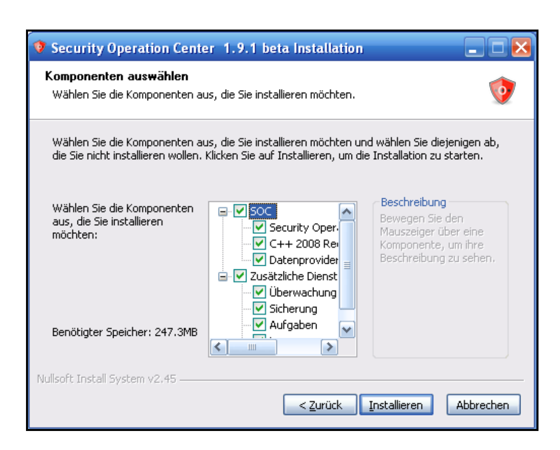


Abb. 2 Installationsassistent des SOC

Das Security Operation Center und der Datenprovider müssen die gleiche Version haben, damit alle Funktionen fehlerfrei ablaufen. Wenn Sie also den Datenprovider aktualisieren, so müssen auch alle Benutzer, die diesen Datenprovider nutzen, das Operation Center aktualisieren.

1.1 Log Center Versionen

Da das Log Center auch Verbindungsdaten der einzelnen Rechner im Netzwerk aufnimmt, kann daraus auf die Internetnutzung jeder Mitarbeiterin/ jedes Mitarbeiters geschlossen werden. Die IP-Adressen und Benutzernamen sind somit für den Administrator sichtbar.

Um personenbezogene Daten vor unberechtigtem Zugang zu schützen, können die Daten der Webreports und des historischen Logs anonymisiert werden. Das heißt, dass IP-Adressen und Benutzernamen für nicht autorisierte Benutzer nicht angezeigt werden. Aus dem gleichen Grund ist für Benutzer ohne Administratorrechte die Schaltfläche ***Log Center*** auch nicht sichtbar.

Sie müssen bei der Installation des Security Operation Centers entscheiden, welche Version des Log Center Sie installieren möchten.
Die Varianten 2-Augen-Prinzip und 4-Augen-Prinzip stehen zur Auswahl.
Beim 2-Augen-Prinzip sind personenbezogene Daten für den Administrator des SOC ohne weitere Autorisierung einsehbar.
Das 4-Augen-Prinzip legt die anonymisierten Daten nur offen, wenn sich der Administrator am Log Center mit einem weiteren Administrator -Account anmeldet. Öffnet der Administrator ohne Eingabe von Benutzername und Kennwort das Log Center, bleiben die personenbezogenen Daten verborgen. Ebenso wenn Anmeldedaten eines „einfachen" Benutzers benutzt werden.
Füllt der Administrator die Anmeldemaske des Log Center mit Benutzername und Kennwort aus, die er auch für die Anmeldung im SOC benutzt, wird der Zugang zum Log Center verwehrt, da das 4-Augen-Prinzip nicht erfüllt ist. Das System prüft nämlich bei eingetragenen Benutzerdaten, ob der Benutzer gleich dem im SOC angemeldeten Benutzer ist und ob der Benutzer Administratorrechte besitzt.



Abb. 3 Auswahl der Log Center Version

1.2 Installation auf Linux Systemen

Sie können das Security Operation Center auch auf Linux Systemen installieren. Allerdings handelt es sich hierbei nur um die grafische Benutzeroberfläche. Es muss eine Verbindung zu einem Datenprovider bestehen, welcher auf einem Windowssystem installiert ist.

Die folgende Installationsanleitung ist für das Betriebssystem Ubuntu getestet. Die Installation auf anderen Linux Betriebssystemen sollte sich ähnlich wenn nicht sogar identisch verhalten.

- Das Operation Center ist als TAR-Archiv erhältlich, welches mit Gzip komprimiert ist.
- Laden Sie die aktuelle Version des SOCs von der Securepoint Seite (http://download.securepoint.de/?d=spopcenter).
  Entpacken Sie das Archiv entweder mit einem Archivmanager oder benutzen Sie die entsprechenden Befehle in einem Terminal.
  Klicken Sie mit der rechten Maustaste auf das Archiv und wählen Sie aus dem Kontextmenü ***Mit dem Archivmanager öffnen***.
- Wählen Sie im Archivmanager den Archivinhalt ***SpOpCenter*** aus und klicken Sie auf ***Entpacken***.
  Das Archiv wird dekomprimiert, entpackt und auf der gleichen Ebene gespeichert.



Abb. 4 Kontextmenü des SOC Archivs

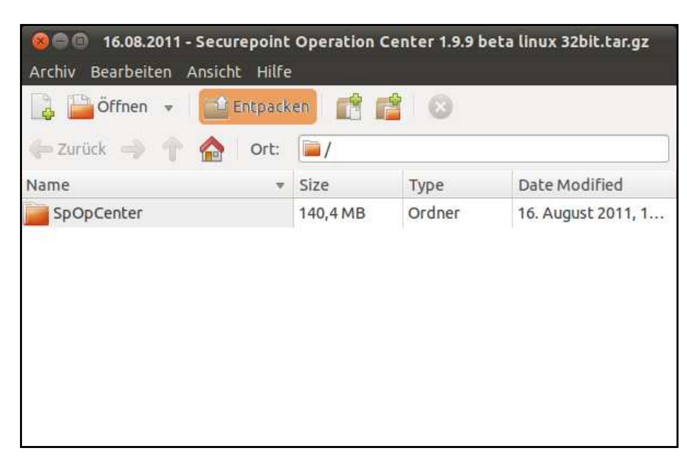


Abb. 5 Entpacken des Archivs

Hinweis: Prüfen Sie vor den nächsten Schritten, ob der ***Desktop*** auch Desktop benannt ist. In neueren Ubuntu Versionen ist dieser Ort nämlich als ***Arbeitsfläche*** benannt. Dann kann die Installationsroutine kein Desktop Icon anlegen. Wenn der Ort als ***Arbeitsfläche*** benannt ist, müssen Sie erst eine ***Verknüpfung für die Arbeitsfläche*** anlegen und diese Verknüpfung in ***Desktop*** umbenennen. Die Verknüpfung muss sich in der gleichen Verzeichnisebene befinden, wie die Arbeitsfläche.

- Öffnen Sie den Ordner ***SpOpCenter*** und starten Sie die Datei ***install.sh*** mit einem Doppelklick.
  Unter Ubuntu wird ein Dialog geöffnet, der abfragt, wie die Datei geöffnet werden soll. Wählen Sie hier ***Im Terminal ausführen***.

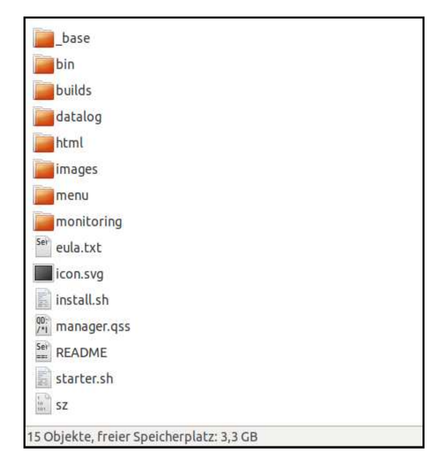


Abb. 6 Inhalt des Ordners SpOpCenter

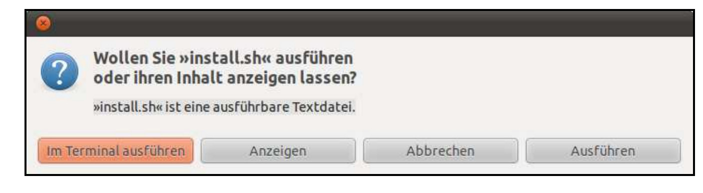


Abb. 7 Abfrage, wie die Datei install.sh geöffnet werden soll.

- Es wird ein Terminal geöffnet in dem die Lizenzbedingungen der Applikation und der verwendeten Module angezeigt werden.
- Wenn Sie diese akzeptieren, geben Sie auf die Abfrage ***Accept***? ein ***Y*** ein und drücken Sie die ***Eingabetaste***.
- Das SOC wird installiert. Nach erfolgter Installation wird das Terminal Fenster geschlossen. Auf dem Desktop sollte die Datei ***starter.sh*** angezeigt werden (Beachten Sie den Hinweis auf der vorherigen Seite).
- Öffnen Sie das Kontextmenü mit einem ***Rechtsklick*** auf diese Datei und wählen Sie den Eintrag ***Eigenschaften***.
- Wechseln Sie im erscheinenden Dialog auf die Registerkarte ***Zugriffsrechte*** und aktivieren Sie die Option ***Datei als Programm ausführen***.
- Klicken Sie auf ***Schließen***. Das Icon für die Datei wurde durch das SOC Icon ersetzt.

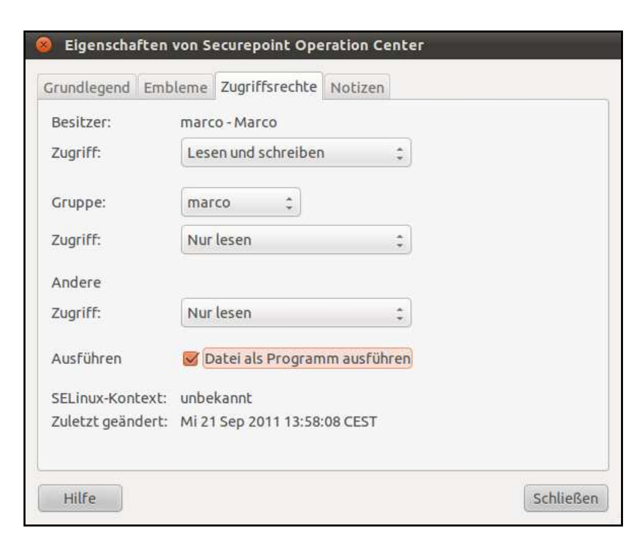


Abb. 8 Ausführmodus ändern

1.3 Installation über ein Terminal

Es wird davon ausgegangen, dass das Operation Center Archiv von der Securepoint Homepage heruntergeladen wurde und auf der Arbeitsfläche des Nutzers abgelegt wurde.

- Starten Sie ein Terminal und wechseln Sie in Ihr ***Homeverzeichnis***.
- Legen Sie mit dem Befehl **`ln -s  Arbeitsfläche Desktop`** einen symbolischen Link auf den Ordner ***Arbeitsfläche*** mit dem Namen ***Desktop*** an, damit ein Icon auf der Arbeitsfläche erstellt werden kann.
- Wechsel Sie jetzt in das Verzeichnis ***Arbeitsfläche***.
- Entpacken Sie das Archiv mit dem Befehl **`tar xfz`**. Wenn Sie eine ausführliche Ausgabe möchten, erweitern Sie die Optionen mit einem **`v`**, also `tar xfzv`.
- Wechsel Sie in den entpackten Ordner ***SpOpCenter*** und starten Sie die Datei ***install.sh***.

```
max@ubuntu-VirtualBox: ~/Arbeitsfläche/SpOpCenter
Datei  Bearbeiten  Ansicht  Suchen  Terminal  Hilfe
max@ubuntu-VirtualBox:~$ pwd
/home/max
max@ubuntu-VirtualBox:~$ ls
Arbeitsfläche  examples.desktop
max@ubuntu-VirtualBox:~$ ln -s Arbeitsfläche Desktop
max@ubuntu-VirtualBox:~$ ls
Arbeitsfläche  Desktop  examples.desktop
max@ubuntu-VirtualBox:~$ cd Arbeitsfläche/
max@ubuntu-VirtualBox:~/Arbeitsfläche$ ls
SOC_Linux.tar.gz
max@ubuntu-VirtualBox:~/Arbeitsfläche$ tar xfz SOC_Linux.tar.gz
max@ubuntu-VirtualBox:~/Arbeitsfläche$ ls
SOC_Linux.tar.gz  SpOpCenter
max@ubuntu-VirtualBox:~/Arbeitsfläche$ cd SpOpCenter/
max@ubuntu-VirtualBox:~/Arbeitsfläche/SpOpCenter$ ls
_base    eula.txt  install.sh    menu        Securepoint Operation Center.sh~
bin      html      install.sh~   monitoring  starter.sh
builds   icon.svg  manager.ini~  README      starter.sh~
datalog  images    manager.qss   README~     sz
max@ubuntu-VirtualBox:~/Arbeitsfläche/SpOpCenter$ ./install.sh
```

Abb. 9 Terminaleingaben bis zum Start der Installation

- Es werden die Lizenzbestimmungen des SOCs und der verwendeten Applikationen gezeigt.
  Schalten Sie mit der ***Leertaste*** zur nächsten Ausgabe.
- Wenn Sie mit den Bedingungen einverstanden sind, geben Sie nach der Frage ***Accept*** ein ***Y*** ein und bestätigen Sie mit der ***Eingabetaste***. Das Operation Center wird nun installiert.

```
 *
 * THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND
 * CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES,
 * INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES
 * OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
 * ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR
 * CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,
 * SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING,
 * BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR
 * SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS
 * INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY,
 * WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING
 * NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE
 * USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY
 * OF SUCH DAMAGE.
 */
Accept? [Y/N]:
Y
```

Abb. 10 Akzeptieren der Lizenzbedingungen

2 Anmelden am Security Operation Center

Nach dem Starten des SOC erscheint ein Login Dialog, mit dem Sie sich am System anmelden müssen. Beim ersten Start verwenden Sie die Standardanmeldedaten:

Benutzername: `admin`
Kennwort: `insecure`

Diese Daten sind ab Werk voreingestellt und sollten nach dem ersten Login geändert werden. Zum Kennwort ändern des Benutzers ***admin*** erscheint nach dem ersten Login automatisch eine Eingabemaske.



Abb. 11 Anmeldedialog

Standardmäßig wird der Datenprovider auf dem lokalen Rechner, also unter der IP-Adresse 127.0.0, abgefragt. Wird hier der Dienst nicht gefunden, muss eine IP-Adresse eines Rechners eingegeben werden, auf dem sich der Dienst befindet. Dazu wird nach einem fehlgeschlagenen Verbindungversuch der Dialog erweitert.

- Geben Sie die ***IP-Adresse*** und den ***Port*** (Standard:6178) des Rechners an.
- Klicken Sie auf ***Test***, um die Verbindung zu prüfen. ***Speichern*** Sie die Einstellung nach erfolgreichem Verbindungsaufbau.
- Melden Sie sich dann mit ***Benutzername*** und ***Kennwort*** an.



Abb. 12 anderen Datenprovider eintragen



Abb. 13 Einstellungen speichern

3 Message Board

Das Message Board zeigt aktuelle Securepoint Nachrichten, Changelogs oder ausgeführte Task an. Das Message Board wird im gesonderten Tab mit der Bezeichnung ***News*** angezeigt. In der oberen Menüleiste kann die Ansicht zwischen den Bereichen ***Neuigkeiten***, ***Changelog***, ***Tasklog*** und ***Nachrichten*** gewechselt werden.
In den Einstellungen des Security Operation Centers kann es als Startseite eingestellt werden, die beim Öffnen des Operation Centers angezeigt wird. In Bereich ***Startseite*** der SOC Einstellungen muss dafür die Einstellung ***Überblick*** gewählt werden.

Die Securepoint ***Neuigkeiten*** informieren über Pressemeldungen und aktuelle Veranstaltungen der Securepoint GmbH. Diese Daten werden von der Securepoint Website geladen und werden somit nur dargestellt, wenn der Rechner auf das Internet zugreifen kann.

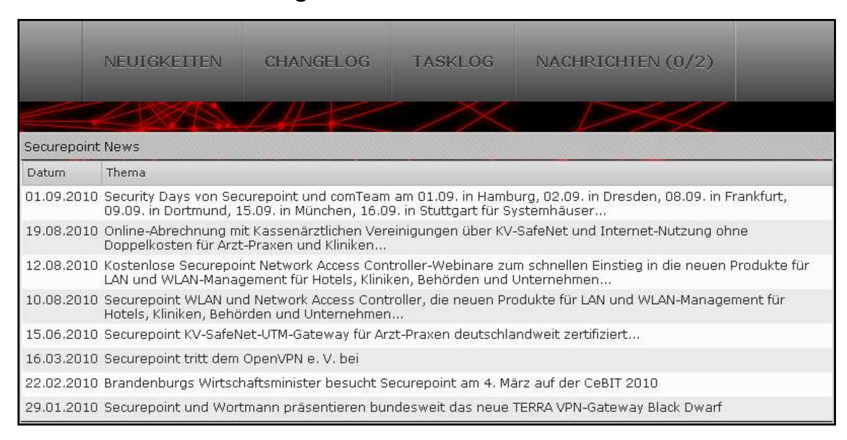


Abb. 14 Neuigkeiten Anzeige des Message Board

Das ***Changelog*** listet die Änderungen zwischen den Versionen der Gateway Software auf. Zur Auswahl der Version steht am Ende der Liste ein Dropdownfeld zur Verfügung.
Auch diese Daten werden direkt aus dem Internet geladen.

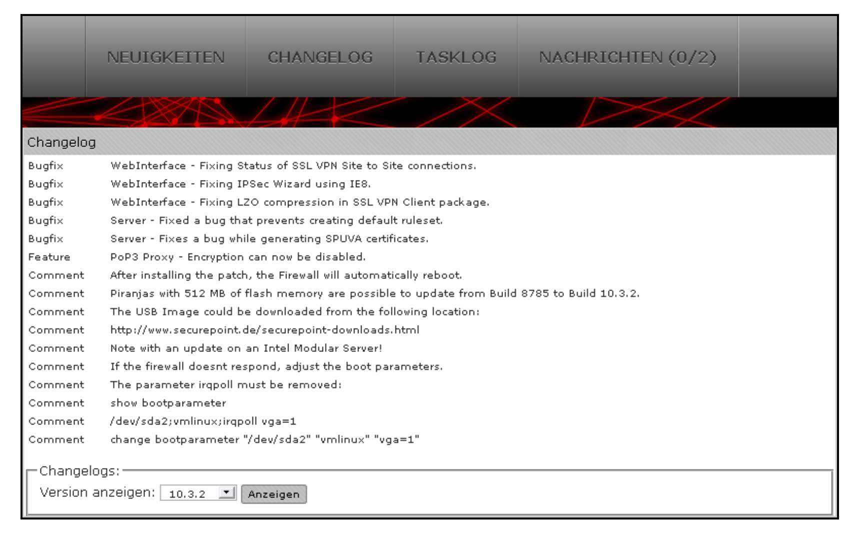


Abb. 15 Changelog Anzeigedes Message Board

Das ***Tasklog*** listet alle ausgeführten Aufgaben auf. Die Einträge beinhalten den Namen der Aufgabe, Ausführungszeitpunkt und Statusmeldung. Mit dem Button am rechten Listenrand kann die jeweilige Meldung ausgeblendet werden. Die Löschung wird automatisch gespeichert und gilt für **alle** Benutzer des Operation Centers.

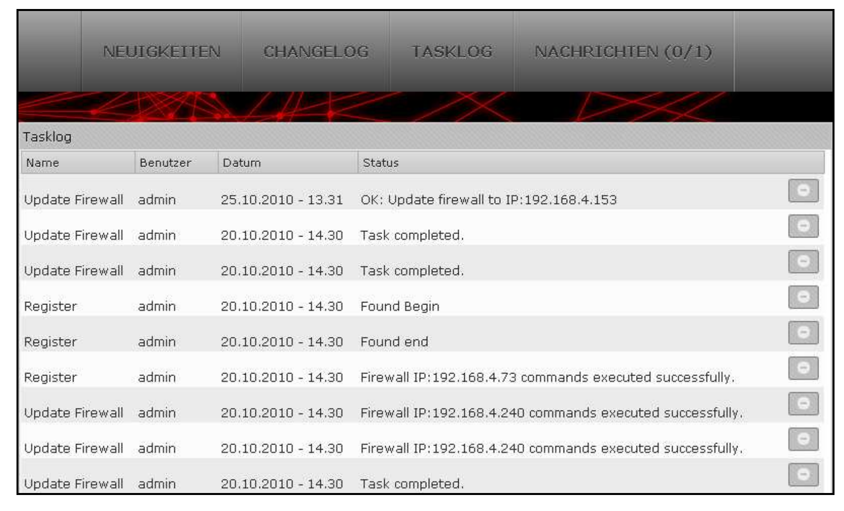


Abb. 16 Tasklog Anzeige des Message Board

Benutzer können einander Nachrichten schreiben. Diese werden im Message Board angezeigt. Benutzer können nur die Nachrichten sehen, die an sie gerichtet sind. Liegen beim Login neue Nachrichten vor, wechselt die Ansicht sofort zum Posteingang.
Gelesene Nachrichten werden automatisch in die Registerkarte ***Gelesene Nachrichten*** verschoben.



Abb. 17 Nachrichten Anzeige des Message Board

4 Monitoring Center

Eine zentrale Funktion des Security Operation Centers ist das ***Monitoring***. Mit dieser Überwachungsfunktion kann die Systemauslastung jeder verwalteten Appliance angezeigt werden. Die Auslastung des Prozessors, des Arbeitsspeichers und der Auslagerungspartition wird grafisch angezeigt. Auch die Anzahl der TCP- und UDP- Verbindungen und der Online/Offline Status werden als Graph dargestellt.
Darunter werden einige Systemkomponenten, Lizenz- und Softwareeigenschaften gelistet. Bei Bedarf können die Listen über gestartete und gestoppte Anwendungen sowie angelegte IPSec-Verbindungen angezeigt werden.

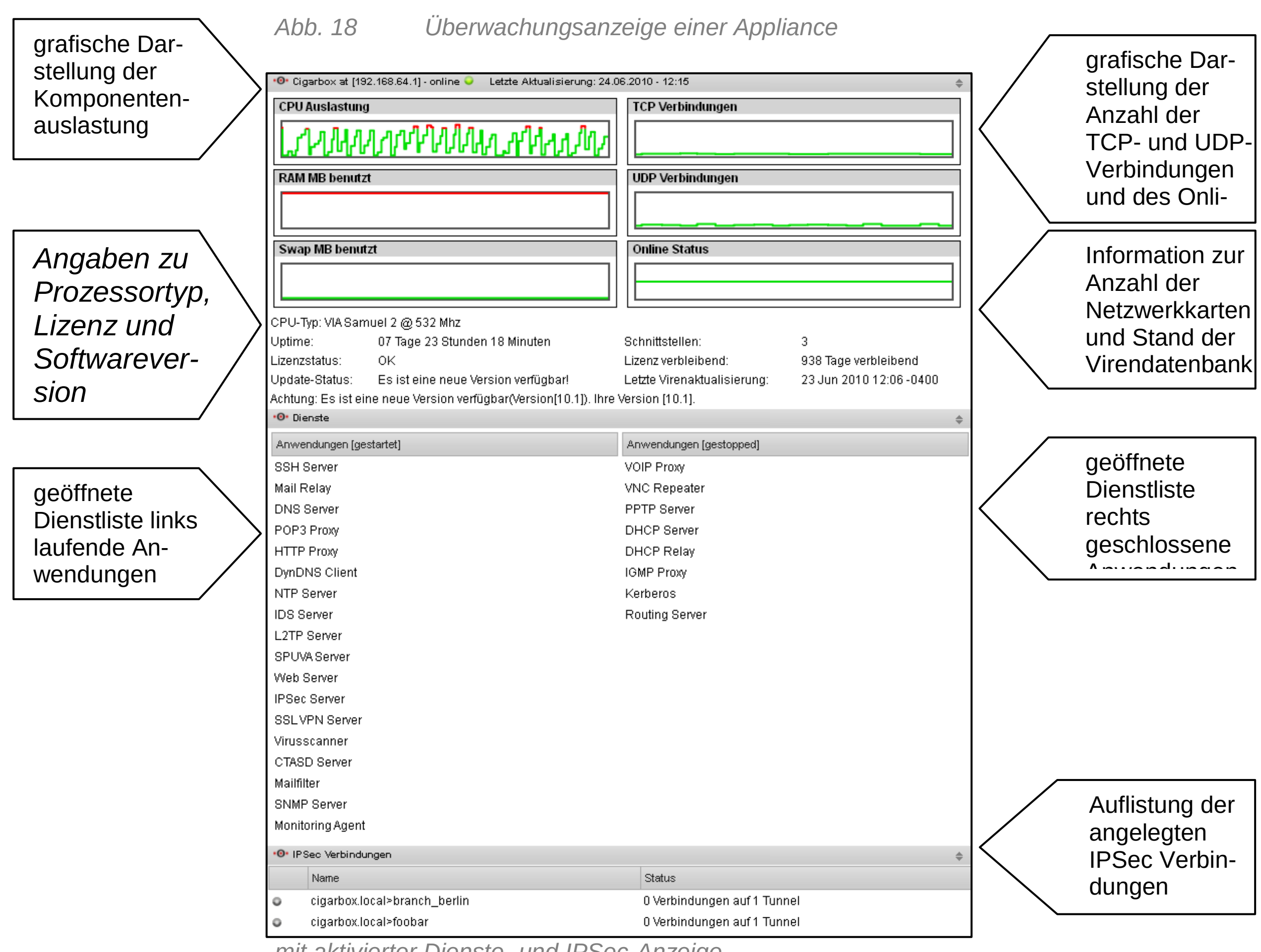


Abb. 18 Überwachungsanzeige einer Appliance mit aktivierter Dienste- und IPSec-Anzeige

4.1 Filter des Monitoring Center

Mit einem Filter können Sie bestimmen, von welchen Appliances die Überwachungsanzeigen dargestellt werden.
Die Filterauswahl finden Sie auf der linken Seite unter dem Punkt ***Monitoring Center***.



Abb. 19 Filter

Filterbezeichnung	Funktion
Anzeigen	Zeigt alle Appliances, außer der exkludierten an.
Alle anzeigen	Zeigt alle Appliances an, auch die exkludierten.
Nur Status exkludiert anzeigen	Zeigt die exkludierten Appliances an.
Nur Status wichtig anzeigen	Zeigt Appliances mit dem Überwachungsstatus *wichtig* an.
Nur Status normal anzeigen	Zeigt Appliances mit dem Überwachungsstatus *normal* an.
Nur Status niedrig anzeigen	Zeigt Appliances mit dem Überwachungsstatus *niedrig* an.
Zeige Gruppe	Öffnet eine weitere Filterauswahl, welche als Filterkriterium die Gruppen anbietet.

Zusätzlich zu diesem Filter können Sie die Ansicht mit der Leiste im unteren Bereich des rechten Fensters anpassen.

- Sie können die aktuelle Ansicht nochmal nach Risiko filtern und nach Name oder Risiko sortieren.
- Es kann in der aktuellen Auswahl nach Appliance-Name oder IP-Adresse gesucht werden.
- Das Aktualisierungsintervall der Anzeige kann stufenweise zwischen 2 Minuten und 4 Stunden gewählt werden.
  - Wird ***Manuell*** gewählt, wird die Anzeige nur aktualisiert, wenn ein Filter auf der linken Seite betätigt wird.
  - Bei der Einstellung ***Überwachung*** wird das Intervall des Monitoring übernommen.
- Die Auswahl kann ein- oder zweispaltig aufgelistet werden.

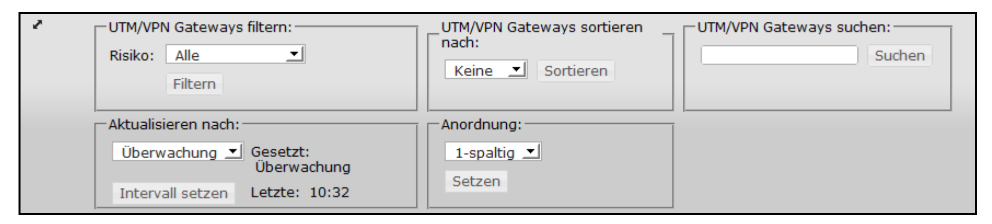


Abb. 20 Ansichtsfilter

4.2 Einstellungen des Monitorings

Die Überwachungsdaten werden nicht ständig von der Appliance angefordert. Es werden so genannte Läufe erstellt. In diesem Lauf werden die Daten der Appliance abgefragt. Es werden bis zu 100 Läufe gespeichert. Das Laufintervall ist die Zeit, die zwischen dem Ende des vorherigen Laufs und dem Start des neuen Laufs verstreicht. In den Standardeinstellungen ist dies eine Minute. Da nur eine Appliance zurzeit und die Appliances nacheinander abgefragt werden, kann die wirklich verstrichene Zeit zwischen den Läufen größer sein.

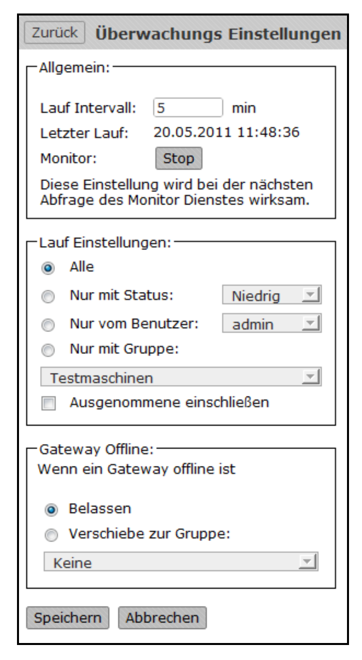


Abb. 21 Einstellungen für das Monitoring

Die Abfragen können für bestimmte Appliances durchgeführt werden.

Zur Auswahl stehen:
- Alle Appliances
- Appliances eines bestimmten Status
- Appliances eines bestimmten Benutzers
- Appliances einer bestimmten Gruppe

Außerdem kann entschieden werden, ob exkludierte Maschinen mit abgefragt werden. Exkludierte Maschinen sind Appliances, die normalerweise vom Monitoring ausgeschlossen sind.

Wird eine abzufragende Appliance im Offline Modus entdeckt, kann diese in eine vorgewählte Gruppe geschoben werden.

5 Dashboard

Sie haben auch die Möglichkeit, die wichtigsten Monitoringdaten im Dashboard anzuzeigen. Das Dashboard zeigt eine grafische Übersicht aller eingetragenen Gateways an. Für jedes Gateway werden die Auslastung der CPU, des Speichers, der Swap Auslagerungspartition und die Gültigkeitsdauer der Lizenz grafisch dargestellt. Außerdem werden die Anzahl der TCP und UDP Verbindung sowie die verwendete Version angezeigt.
Das Dashboard kann in Boxen oder als Liste angezeigt werden.

Die farbliche Hinterlegung des Gateway-Namens bzw. der Listenzeile gibt schnell Auskunft über kritische Systeme.
Eine rote Hinterlegung signalisiert, dass das Risiko des Systems als hoch bewertet wird. Dies ist der Fall, wenn z. B. das System nicht erreichbar bzw. nicht eingeschaltet ist oder die Lizenz abgelaufen ist oder die Lizenz weniger als 30 Tage gültig ist und eine alte Version verwendet wird.
Eine orange Markierung wird gezeigt, wenn eine veraltete Version verwendet wird.
Ist der Name grün hinterlegt, befindet sich das System im unkritischen Zustand.
Auch die Statusbalken der momentanen Auslastung ändern die Farbe, wenn sie in einen kritischen Bereich kommen.

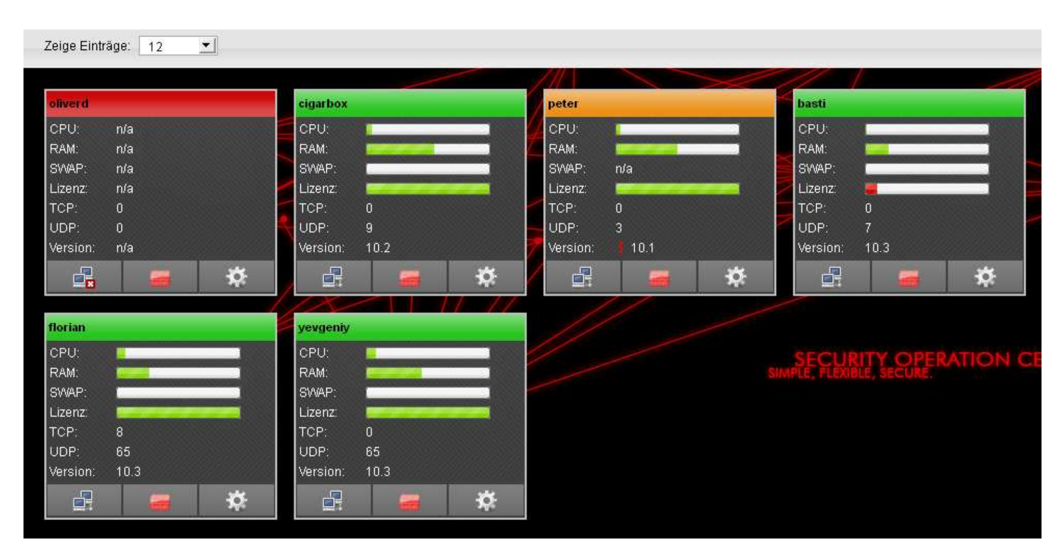
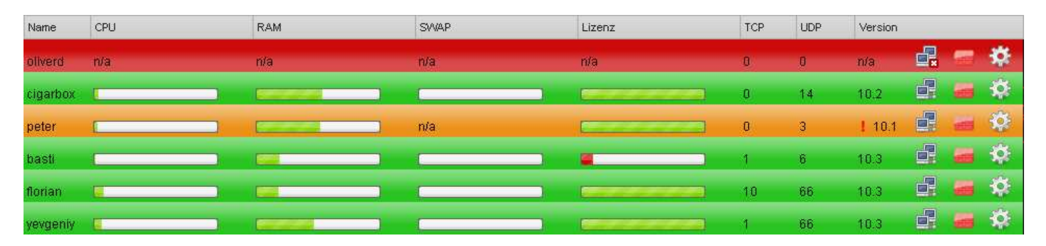


Abb. 22 Dashboard in Boxenansicht



Name	CPU	RAM	SWAP	Lizenz	TCP	UDP	Version
oliverd	n/a	n/a	n/a	n/a	0	0	n/a
cigarbox					0	14	10.2
peter			n/a		0	3	! 10.1
basti					1	6	10.3
florian					10	66	10.3
yevgeniy					1	66	10.3

Abb. 23 Dashboard in Listenansicht

Die Icons am unteren Rand der Box bzw. am Ende der Liste zeigen den Verbindungsstatus, weitere Details oder bauen eine Verbindung zum Gateway auf.

Icon	Bedeutung
	Gateway ist zum Monitoring-Zeitpunkt nicht erreichbar, nicht eingeschaltet oder nicht verbunden.
	Verbindung zum Gateway ist herge-stellt.
	Mit dem Administrations-Webinterface des Gateway verbinden.
	Details des Gateway anzeigen.

5.1 Details

Mit einem Klick auf das ***Zahnradsymbol*** werden nähere Informationen des jeweiligen Sys-tems angezeigt.

Die Registerkarte ***Allgemein*** zeigt Informationen zur Hardware, Lizenz, Softwareversion und Virendatenbankstand an.



Abb. 24 Details - Registerkarte Allgemein

Auf der Registerkarte ***Dienste*** sind alle laufenden und gestoppten Anwendungen getrennt aufgelistet.

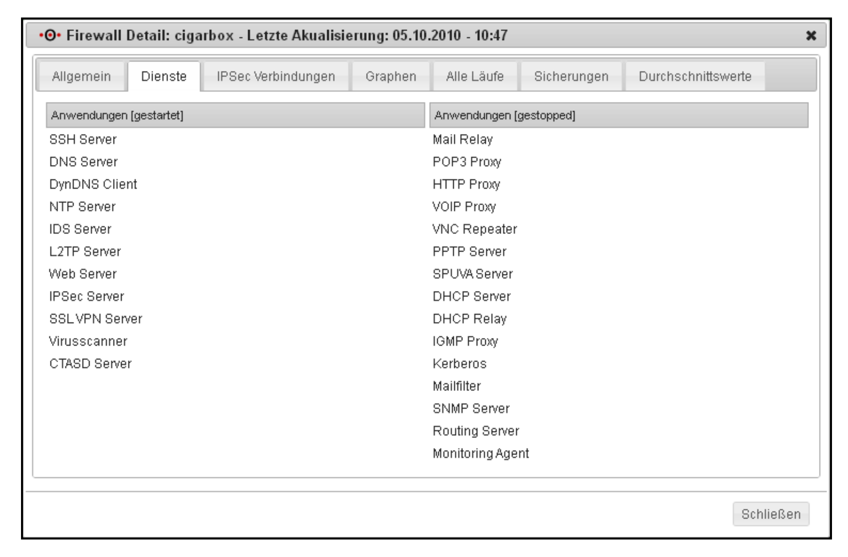


Abb. 25 Details - Registerkarte Dienste

Die Registerkarte ***IPSec Verbindungen*** zeigt die auf dem Gateway eingerichteten IPSec Verbindungen an. In der ersten Spalte wird der Status der Verbindung durch einen Punkt dargestellt. Ist die Verbindung aktiv, ist der Punkt grün, ansonsten ist der Punkt grau.

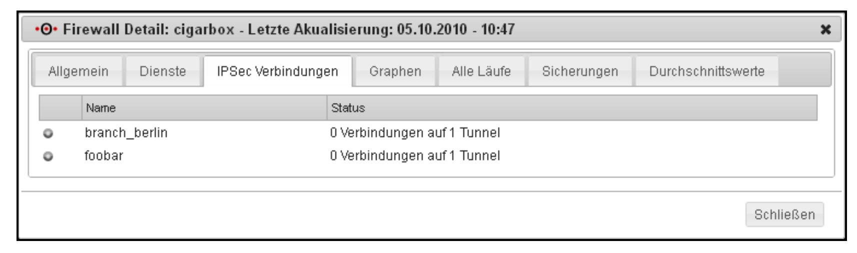


Abb. 26 Details - Registerkarte IPSec Verbindungen

Die Registerkarte ***Graphen*** zeigt die Hardwareauslastung sowie die Anzahl der TCP- und UDP-Verbindungen und den Online Status in Diagrammen an.

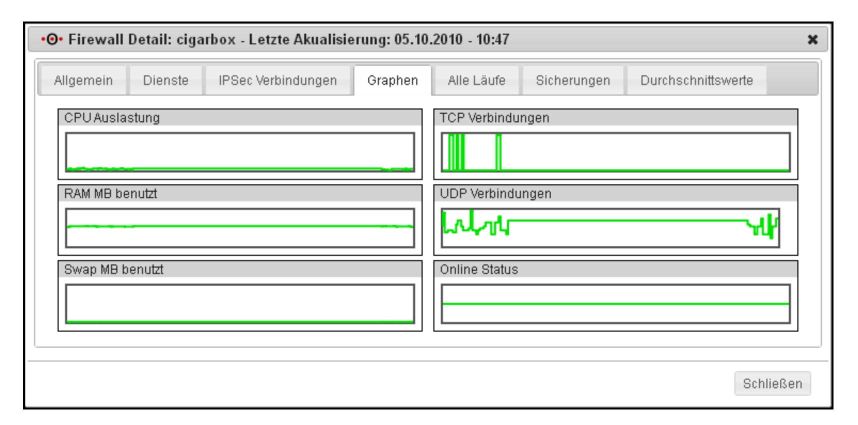


Abb. 27 Details - Registerkarte Graphen

Auf der Registerkarte ***Alle Läufe*** werden der Aufnahmezeitpunkt der letzten 100 Statusaufzeichnungsläufe mit Datum und Uhrzeit aufgelistet. Durch Anklicken des Buttons am Zeilenende können genauere Informationen zu jedem Lauf aufgerufen werden.

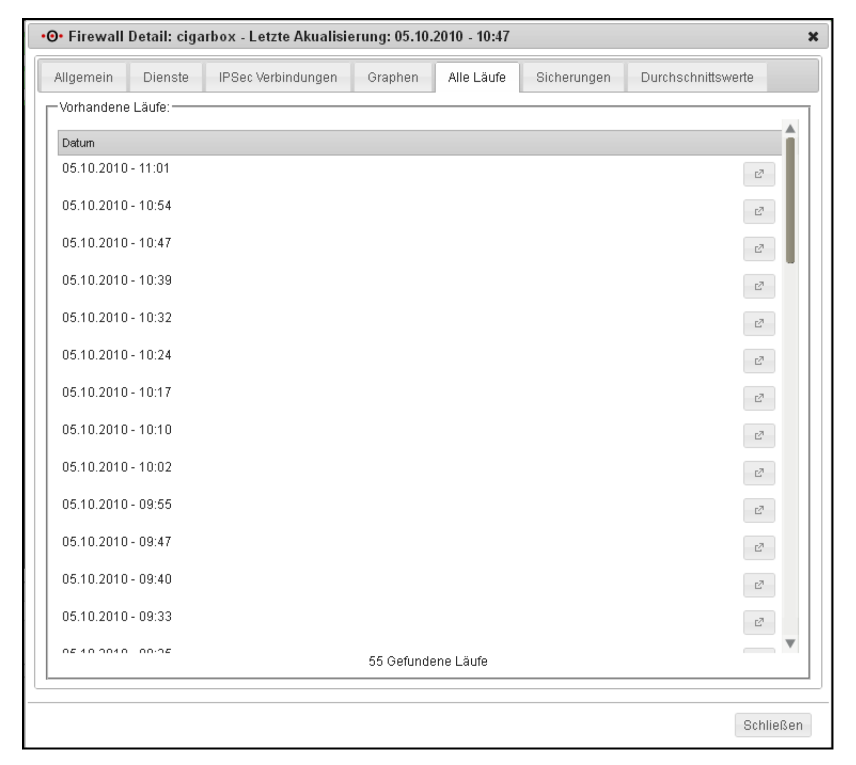


Abb. 28 Details - Registerkarte Alle Läufe

Auf der Registerkarte ***Sicherungen*** werden nähere Informationen zu den letzten Backups angezeigt.



Abb. 29 Details - Sicherungen

Die Registerkarte ***Durchschnittswerte*** zeigt die rechnerischen Durchschnitte der Hardware-auslastung, der Anzahl der TCP- und UDP-Verbindungen und des Online-Status.

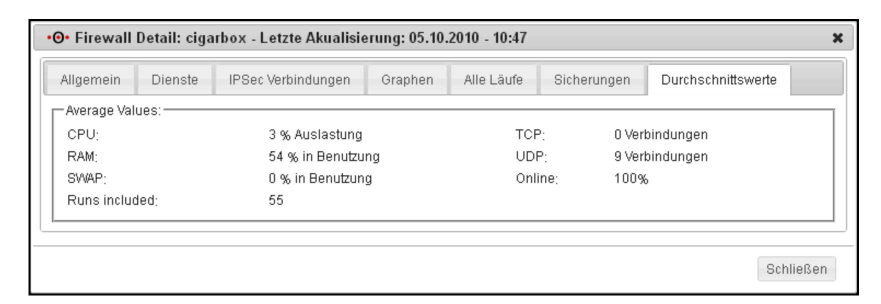


Abb. 30 Details - Registerkarte Durchschnittswerte

5.2 Ansichtsfilter des Dashboards

Auch die Dashboard-Ansicht kann durch einen Filter angepasst werden.
Nach Einstellung des gewünschten Filters, muss noch der jeweilige Button gedrückt werden, um die Filterung und/oder Sortierung zu starten. Auf Wunsch kann die eingestellte Darstellung gespeichert werden.

Bezeichnung	**Funktion**
UTM/VPN Gateways filtern	Die Anzeige des Dashboards kann nach dem Risiko des Gateways gefiltert werden. Es wird unterschieden zwischen kein, mittleres und hohes Risiko. Bei der Einstellung alle wird keine Einschränkung vorgenommen.
UTM/VPN Gateways sortieren	Es kann nach Name und Risiko sortiert werden. Dabei kann zwischen aufsteigender und absteigender Anzeige gewählt werden.
UTM/VPN Gateway suchen	Eine Suche nach Namen oder IP-Adresse eines Gateways kann ausgeführt werden. Ist die Suche erfolgreich, wird die entsprechende Box angezeigt.
Ansicht	Wechselt die Anzeige von Galerie- auf Listenansicht.
Aktualisieren nach	Setzen des Aktualisierungsintervalls der Anzeige. Bei der Einstellung Manuell wird die Anzeige nur aktualisiert, wenn ein Filter im linken Fenster geändert wird. Steht der Wert auf Überwachung, wird das Überwachungsintervall übernommen, das im linken Fenster unter Einstellungen gesetzt ist.
Einstellungen speichern	Speichert die aktuellen Einstellungen für den Clientrechner.

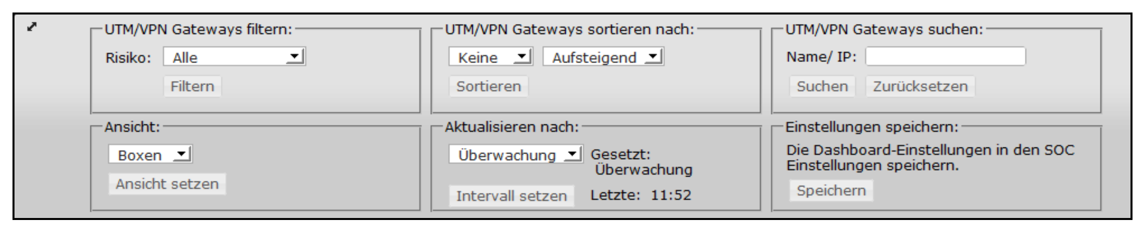


Abb. 31 Filter für das Dashboard

6 Extras

In dem Bereich ***Extras*** können Gateway-Gruppen, Benutzergruppen und Benutzer verwaltet werden. Außerdem kann eine Liste aller im System befindlichen Firewalls und deren Eigenschaften abgerufen werden. Von hier erreichen Sie auch die Punkte Aufgaben, Aufgaben Log und Protokollierung.

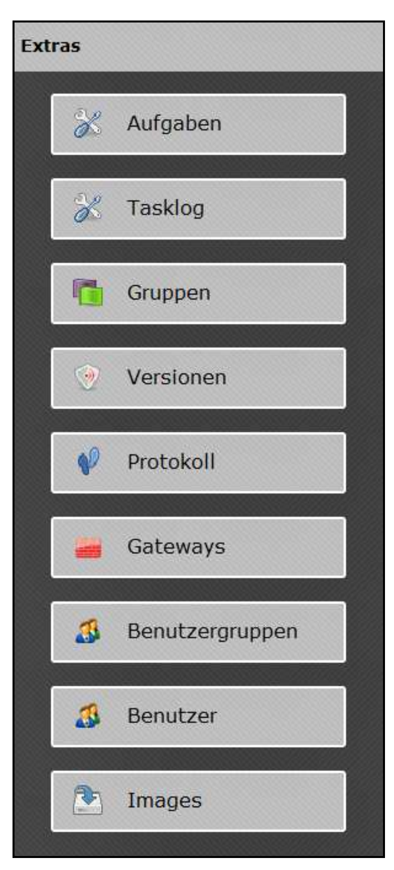


Abb. 32 Menü Extras

6.1 Aufgaben

Unter dem Punkt ***Aufgaben*** können Sie CLI Befehle für Firewalls einrichten, die zu einem bestimmten Zeitpunkt ausgeführt werden.

Unter diesem Punkt finden Sie das Fenster ***Aufgaben verwalten***, in dem alle angelegten Aufgaben mit Namen und Ausführungszeitpunkt aufgeführt sind. Es werden auch schon ausgeführte Aufgaben angezeigt. Da Aufgaben nur zu einem Zeitpunkt durchgeführt werden, haben Sie hier Vorlagen für Aufgaben, die regelmäßig durchgeführt werden.
Der Benutzer ***admin*** kann alle Aufgaben einsehen.

6.1.1 Aufgabe bearbeiten

- Um Aufgaben zum neuen Zeitpunkt oder für andere Gateways auszuführen, benutzen Sie das ***Werkzeugschlüsselsymbol***.
  Es öffnet das Fenster ***Aufgabe bearbeiten***.
- Ändern Sie hier das ***Laufdatum*** und die ***Laufzeit***.
- Ändern Sie ggf. die Gateways, auf denen die Aufgabe ausgeführt werden soll. Nutzen Sie dazu den Button ***Hinzufügen*** im Bereich ***Zugewiesene Gateways***. Wählen Sie dann aus einer Liste die gewünschten Gateways.
- Klicken Sie abschließend auf ***Speichern***.

- Sie können die Aufgaben mit dem ***Abfalleimersymbol*** von der Liste löschen.



Abb. 33 Aufgabenliste

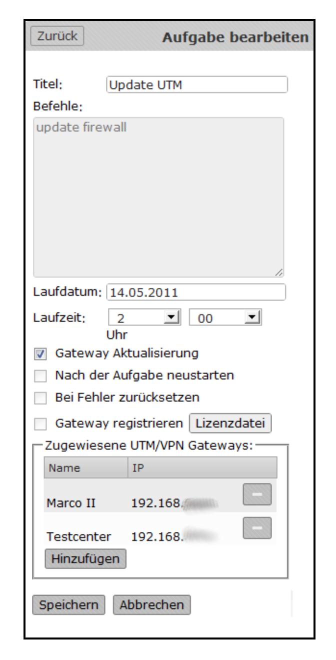


Abb. 34 Aufgabe bearbeiten

6.1.2 Aufgabe erstellen

- Um eine neue Aufgabe zu erstellen, klicken Sie in der Ansicht ***Aufgaben Verwalten*** auf den Button ***Hinzufügen***.
  Es erscheint die Ansicht ***Aufgaben hinzufügen***.
- Tragen Sie im Feld ***Titel*** einen Namen für die Aufgabe ein.
- Geben Sie CLI Befehle im Textfeld ***Befehle*** ein (siehe CLI-Referenz auf der Securepoint Internetseite).
  Die Befehle ***Gateway aktualisieren*** und ***Gateway registrieren*** sind vordefiniert und können per Checkbox aktiviert werden.
- Klicken Sie in das Feld ***Laufdatum***. Es öffnet sich ein Kalender, von dem Sie ein Datum für die Ausführung auswählen können.
- Bei ***Laufzeit*** wählen Sie im ersten Dropdownfeld die Stunden und im zweiten die Minuten der Ausführung.
- Neben den vordefinierten Befehlen ***Gateway aktualisieren*** und ***Gateway registrieren*** sind noch optional ***Neustart*** und ***Zurücksetzen*** wählbar.
  Die Option ***Bei Fehler zurücksetzen*** sollten Sie aktiviert lassen, um fehlgeschlagene CLI Kommandos rückgängig zu machen.
- Klicken Sie auf ***Speichern***.
- Es erscheint die Ansicht ***Aufgaben Gateways***. Die im System eingetragenen Gateways sind hier mit Namen und IP-Adresse aufgelistet.
- Wählen Sie aus, für welche Gateways die Aufgabe ausgeführt werden soll. Klicken Sie dafür auf den Button mit dem ***Plussymbol***.
- Wenn Sie die gewünschten Gateways der Aufgabe zugeordnet haben, klicken Sie auf ***Zurück***.

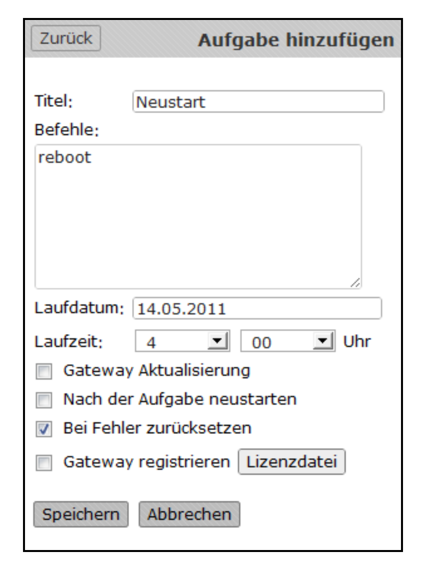


Abb. 35 neue Aufgabe erstellen

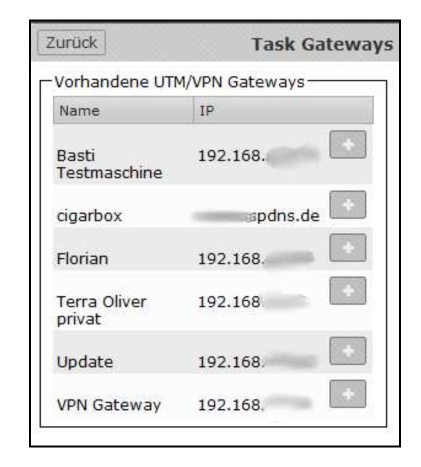


Abb. 36 Gateways auswählen

6.1.3 Makros erstellen

Sie können auch CLI Befehle direkt bei der Administration einer Firewall als Makro aufzeichnen. Die Funktion ist nützlich, wenn Sie auf mehreren Firewalls die gleichen Aktionen ausführen wollen oder wiederkehrende Aufgaben automatisieren möchten.
Wenn Sie sich mit einer Firewall verbinden, können Sie über das Kontextmenüeintrag ***Start Makro*** CLI Befehlen aufzeichnen.
Wenn die Aufnahme gestartet ist, werden Befehle, die im Administrations-Webinterface abgesetzt werden, aufgezeichnet. Dies betrifft allerdings nur Befehle, die Daten ändern, Dienste aktualisieren, neu starten und stoppen. Wird die Protokollierung beendet, können die aufgezeichneten Befehle als Aufgabe gespeichert werden. Diese kann gleich bei der Speicherung mit einem Ausführungstermin versehen werden.

6.1.3.1 Makro aufzeichnen

- Verbinden Sie sich mit der Firewall, bei der Sie ein Makro anlegen wollen.
- Öffnen Sie im Verbindungsfenster mit der rechten Maustaste das Kontextmenü.
- Klicken Sie zum Starten der Aufzeichnung auf den Eintrag ***Start Makro***. Alle CLI-Befehle, die im Administrations-Webinterface ausgeführt werden, werden jetzt aufgezeichnet. Die Anzahl der aufgezeichneten Befehle werden im Makrodialog angezeigt.
- Zum Beenden der Aufzeichnung klicken Sie auf den Eintrag ***Stopp Makro*** .

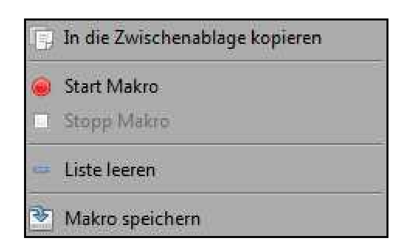


Abb. 37 Kontextmenü mit Makro Einträgen

6.1.3.2 Makro speichern

- Durch das Beenden der Makroaufzeichnung wird der Eintrag ***Makro Speichern*** aktiviert.
  Klicken Sie auf diesen, um das Aufzeichnungsfenster zu öffnen. Hier sind die aufgezeichneten Befehle gelistet. Sie können die Befehle bearbeiten, indem Sie mit der Maus in das Textfeld klicken und mit der Tastatur Änderungen vornehmen.
- Zum Abspeichern geben Sie im Feld ***Titel*** einen Namen für das Makro ein.
- Wählen Sie im Bereich ***Lauf Datum/Zeit*** aus dem Dropdownfeld ein Datum und tippen Sie die gewünschte Uhrzeit ein.
- Sie können noch die Aktionen ***Neustarten nach ausführen*** und ***Rollback bei Fehler*** (Bei einem Fehler die Befehle zurücksetzen) aktivieren.
- Klicken Sie auf ***Speichern***, um das Makro zu speichern.
  Das Makro wird als Aufgabe in der Aufgabenverwaltung angezeigt.

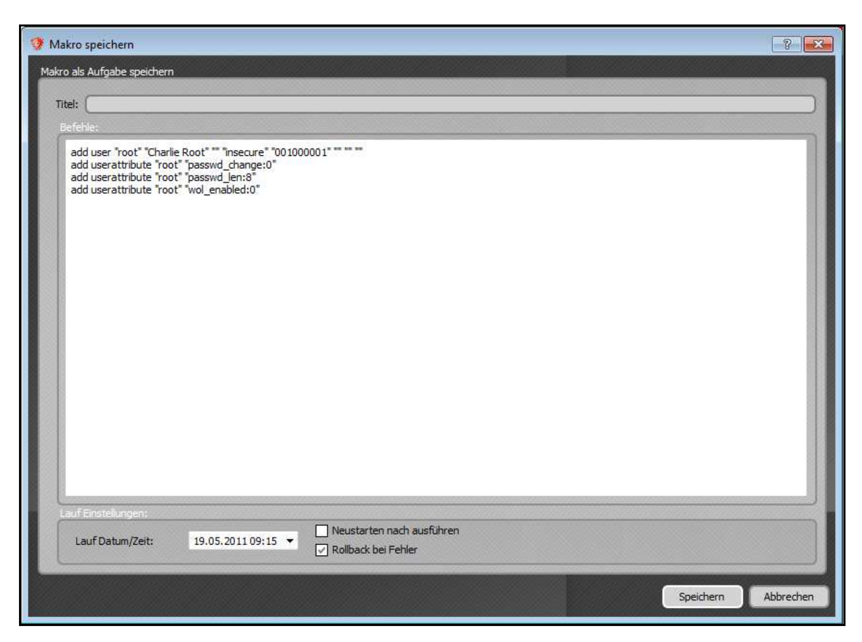


Abb. 38 Makro als Aufgabe speichern

6.2 Tasklog

Im Tasklog finden Sie Protokollierungen der ausgeführten Aufgaben. So können Sie überprüfen, ob die angelegten Aufgaben ordnungsgemäß durchgeführt worden sind oder Fehler aufgetreten sind.
Eintragungen werden solange vorgehalten, bis sie als gelesen markiert sind. Wird der Status durch den Button mit dem ***Minussymbol*** auf gelesen gesetzt, werden die entsprechenden Einträge gelöscht.
Die Einträge sind aufsteigend nach dem Ausführungszeitpunkt aufgelistet und mit dem Namen der Aufgabe versehen. In der dritten Spalte sind die Rückmeldungen des Systems gelistet. Durch den Button in der vierten Spalte kann der jeweilige Eintrag gelöscht werden.

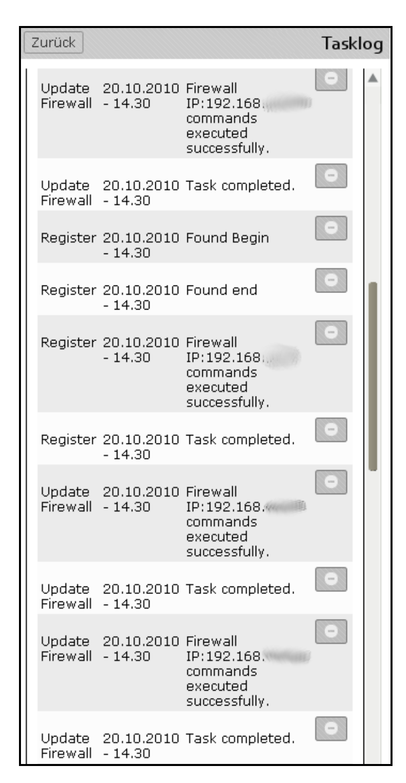


Abb. 39 Statusberichte ausgeführter Aufgaben

6.3 Gruppenverwaltung

In diesem Bereich werden Gruppen verwaltet, denen die Firewalls zugeordnet werden. Sie dienen der Einteilung aller Firewalls in logische Einheiten. In Gruppen erster Ordnung können Sie Untergruppen anlegen.
Gruppen werden auch als Filterauswahl in der Auflistung der Appliances im Bereich ***UTM/VPN Gateway Center*** und beim Monitoring benutzt.

Sie können über die Schaltfläche in den einzelnen Zeilen Gruppen bearbeiten oder löschen.

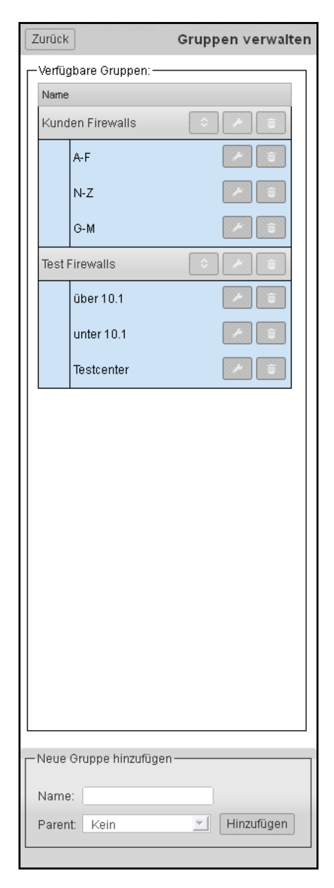


Abb. 40 Liste aller Gruppen

Im unteren Bereich können Sie neue Gruppen anlegen. Hierbei entscheiden Sie, ob es sich um eine Gruppe erster Ordnung oder eine Untergruppe handelt.

- Geben Sie im Feld ***Namen*** die Bezeichnung für die Gruppe ein.
- Wählen Sie im Feld ***Parent*** in welcher Gruppe 1. Ordnung die Gruppe als Untergruppe angelegt werden soll. Handelt es sich um eine ***Hauptgruppe***, wählen Sie den Eintrag ***Kein*** aus.
- Klicken Sie auf ***Hinzufügen***.

Mit dem ***Werkzeugschlüssel*** Symbol hinter jeder Gruppe können Sie den Namen der jeweiligen Gruppe ändern. Für Untergruppen können Sie auch die Hauptgruppe wechseln oder die Gruppe selbst zur Hauptgruppe machen. Hauptgruppen, die Untergruppen beinhalten, können nicht zu Untergruppen werden.

Gruppen können Sie mit dem ***Abfalleimer*** Symbol löschen. Beinhaltende Firewalls bleiben dabei bestehen.
Löschen Sie eine Untergruppe werden die Firewalls in die Hauptgruppe verschoben. Löschen Sie eine Hauptgruppe werden ebenfalls alle Untergruppen gelöscht und die Firewalls sind keiner Gruppe mehr zugeordnet.

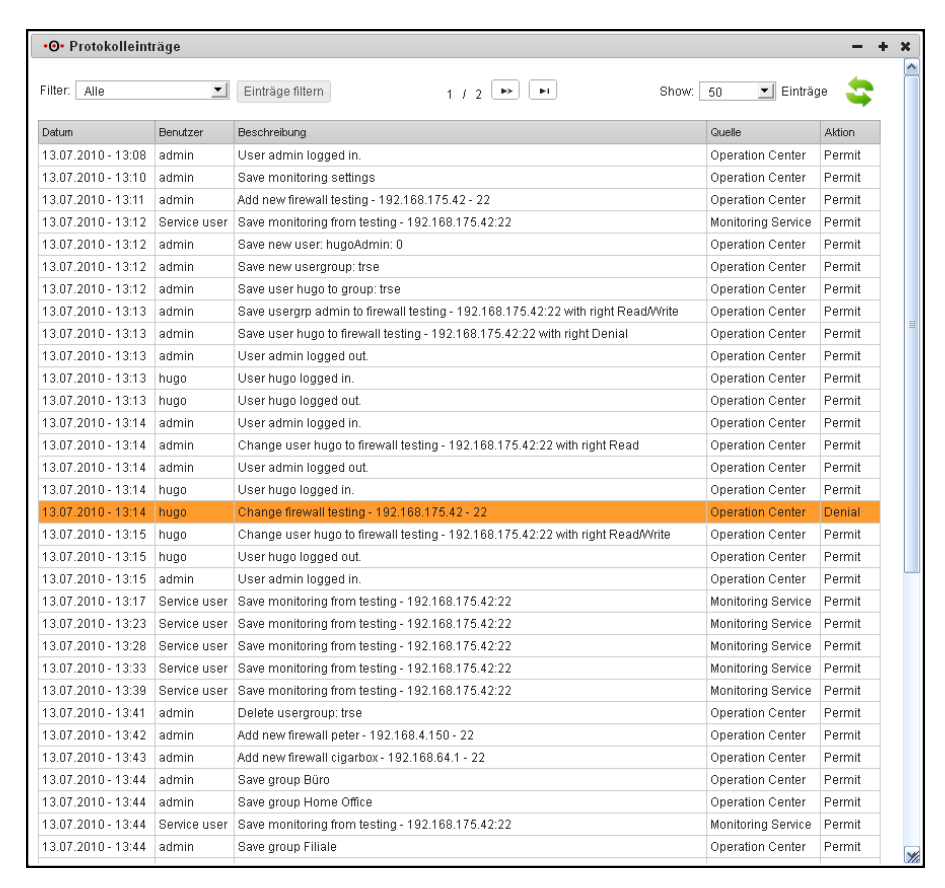
6.4 Versionen

Hier können Sie sich über die verfügbaren Versionen der Firewall-Software informieren. Wenn eine neue Version vorliegt, wird beim Verbinden zu einer Firewall, die eine alte Version verwendet, eine Meldung angezeigt, die Ihnen die Möglichkeit bietet, die neue Version herunterzuladen.

6.5 Protokoll

Unter dem Punkt ***Protokoll*** werden Ihnen Protokolleinträge angezeigt, die vom Dienst Data Provider automatisch angelegt werden. Es werden alle Bedienungen protokolliert, die ein Benutzer am Security Operation Center durchführt. Zusätzlich werden Aktionen wie das Erstellen von Sicherungen und Monitoringläufen des Systems protokolliert.
So kann nachverfolgt werden, welche Aktionen von den Benutzern und dem System ausgeführt worden sind.

Das Protokoll ist nur für Benutzer mit Administratorrechten einsehbar.
In der Anzeige werden die Aktionen als ***Permit*** (Zulassung) oder ***Denial*** (Verweigerung) gekennzeichnet. Wurde von einem Benutzer mit eingeschränkten Rechten versucht, privilegierte Aktionen auszuführen, wird dies mit dem Eintrag ***Denial*** angezeigt. Zusätzlich wird die betreffende Zeile durch eine farbige Unterlegung gekennzeichnet.



Datum	Benutzer	Beschreibung	Quelle	Aktion
13.07.2010 - 13:08	admin	User admin logged in.	Operation Center	Permit
13.07.2010 - 13:10	admin	Save monitoring settings	Operation Center	Permit
13.07.2010 - 13:11	admin	Add new firewall testing - 192.168.175.42 - 22	Operation Center	Permit
13.07.2010 - 13:12	Service user	Save monitoring from testing - 192.168.175.42:22	Monitoring Service	Permit
13.07.2010 - 13:12	admin	Save new user: hugoAdmin: 0	Operation Center	Permit
13.07.2010 - 13:12	admin	Save new usergroup: trse	Operation Center	Permit
13.07.2010 - 13:12	admin	Save user hugo to group: trse	Operation Center	Permit
13.07.2010 - 13:13	admin	Save usergrp admin to firewall testing - 192.168.175.42:22 with right Read/Write	Operation Center	Permit
13.07.2010 - 13:13	admin	Save user hugo to firewall testing - 192.168.175.42:22 with right Denial	Operation Center	Permit
13.07.2010 - 13:13	admin	User admin logged out.	Operation Center	Permit
13.07.2010 - 13:13	hugo	User hugo logged in.	Operation Center	Permit
13.07.2010 - 13:13	hugo	User hugo logged out.	Operation Center	Permit
13.07.2010 - 13:14	admin	User admin logged in.	Operation Center	Permit
13.07.2010 - 13:14	admin	Change user hugo to firewall testing - 192.168.175.42:22 with right Read	Operation Center	Permit
13.07.2010 - 13:14	admin	User admin logged out.	Operation Center	Permit
13.07.2010 - 13:14	hugo	User hugo logged in.	Operation Center	Permit
13.07.2010 - 13:14	hugo	Change firewall testing - 192.168.175.42 - 22	Operation Center	Denial
13.07.2010 - 13:15	hugo	Change user hugo to firewall testing - 192.168.175.42:22 with right Read/Write	Operation Center	Permit
13.07.2010 - 13:15	hugo	User hugo logged out.	Operation Center	Permit
13.07.2010 - 13:15	admin	User admin logged in.	Operation Center	Permit
13.07.2010 - 13:17	Service user	Save monitoring from testing - 192.168.175.42:22	Monitoring Service	Permit
13.07.2010 - 13:23	Service user	Save monitoring from testing - 192.168.175.42:22	Monitoring Service	Permit
13.07.2010 - 13:28	Service user	Save monitoring from testing - 192.168.175.42:22	Monitoring Service	Permit
13.07.2010 - 13:33	Service user	Save monitoring from testing - 192.168.175.42:22	Monitoring Service	Permit
13.07.2010 - 13:39	Service user	Save monitoring from testing - 192.168.175.42:22	Monitoring Service	Permit
13.07.2010 - 13:41	admin	Delete usergroup: trse	Operation Center	Permit
13.07.2010 - 13:42	admin	Add new firewall peter - 192.168.4.150 - 22	Operation Center	Permit
13.07.2010 - 13:43	admin	Add new firewall cigarbox - 192.168.64.1 - 22	Operation Center	Permit
13.07.2010 - 13:44	admin	Save group Büro	Operation Center	Permit
13.07.2010 - 13:44	admin	Save group Home Office	Operation Center	Permit
13.07.2010 - 13:44	Service user	Save monitoring from testing - 192.168.175.42:22	Monitoring Service	Permit
13.07.2010 - 13:44	admin	Save group Filiale	Operation Center	Permit

Abb. 41 Protokollanzeige

6.5.1 Anpassung der Protokollanzeige

Im Kopf des Dialogs ist ein Filter integriert, mit dem Sie die Ansicht anpassen können. Nachdem Sie einen Filter gewählt haben, klicken Sie auf den Button ***Einträge filtern***, um die Anzeige zu aktualisieren.

Folgende Filterungen werden angeboten:

- Alle Zeigt alle Protokolleinträge an.
- Operation Center Zeigt Einträge des Operation Centers. Dies sind die Aktionen, die Benutzer im Operation Center ausgeführt haben.
- Überwachungsdienst Einträge über durchgeführte Monitoringläufe.
- Sicherungsdienst Einträge über erstellte Konfigurationssicherungen.

In der Mitte der Kopfleiste haben Sie die Möglichkeit, durch die Protokollseiten zu navigieren. Die Anzahl der Einträge pro Seite ist standardmäßig auf 20 gesetzt. Sie können im rechten Dropdownfeld die Anzahl der Einträge anpassen.

Am rechten Rand befindet sich ein Button mit zwei grünen Pfeilen , mit dem Sie die Einträge aktualisieren können.



Abb. 42 Kopfleiste des Dialogs Protokolleinträge

6.5.2 Protokoll Einstellungen

Dieser Punkt befindet sich unter dem Menü ***Operation Center***.

Hier können Sie bestimmen, wie viele Tage die Protokolleinträge vorgehalten werden. Protokolldaten, die älter sind als die ausgewählte Zeit, werden gelöscht.

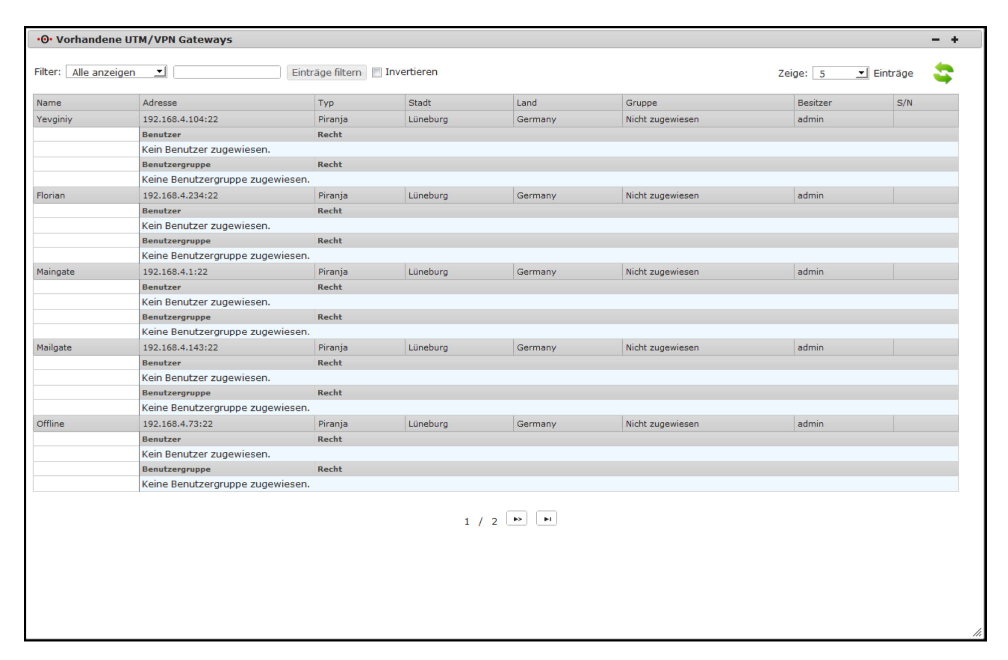
Sie können die Daten bis zu 30 Tage speichern. Die Anzahl der Einträge ist hierbei unerheblich.



Abb. 43 Vorhaltezeit in Tagen

6.6 UTM/VPN Gateways

Der Punkt ***UTM/VPN Gateways*** im Menü ***Extras*** listet Ihnen alle verwalteten Gateways auf. Die Liste enthält den Namen und die IP-Adresse oder den Hostnamen des Gateway. Weiterhin sind noch Gateway-Typ, Standort und Besitzer des Systems angegeben. Auch Benutzer und Benutzergruppen und deren Rechte werden angezeigt, soweit diese vorhanden sind.



Name	Adresse	Typ	Stadt	Land	Gruppe	Besitzer	S/N
Yevginiy	192.168.4.104:22	Piranja	Lüneburg	Germany	Nicht zugewiesen	admin	
	Benutzer	**Recht**					
	Kein Benutzer zugewiesen.						
	Benutzergruppe	**Recht**					
	Keine Benutzergruppe zugewiesen.						
Florian	192.168.4.234:22	Piranja	Lüneburg	Germany	Nicht zugewiesen	admin	
	Benutzer	**Recht**					
	Kein Benutzer zugewiesen.						
	Benutzergruppe	**Recht**					
	Keine Benutzergruppe zugewiesen.						
Maingate	192.168.4.1:22	Piranja	Lüneburg	Germany	Nicht zugewiesen	admin	
	Benutzer	**Recht**					
	Kein Benutzer zugewiesen.						
	Benutzergruppe	**Recht**					
	Keine Benutzergruppe zugewiesen.						
Mailgate	192.168.4.143:22	Piranja	Lüneburg	Germany	Nicht zugewiesen	admin	
	Benutzer	**Recht**					
	Kein Benutzer zugewiesen.						
	Benutzergruppe	**Recht**					
	Keine Benutzergruppe zugewiesen.						
Offline	192.168.4.73:22	Piranja	Lüneburg	Germany	Nicht zugewiesen	admin	
	Benutzer	**Recht**					
	Kein Benutzer zugewiesen.						
	Benutzergruppe	**Recht**					
	Keine Benutzergruppe zugewiesen.						

Abb. 44 Liste aller verwalteten Gateways

6.6.1 Filter der Gateway-Liste

Im Kopf der Tabelle ist ein Filter für die Anzeige enthalten. Hiermit können Sie die Liste nach bestimmten Gateways filtern, die Anzahl der Einträge pro Seite bestimmen und die Einträge aktualisieren.

Als Filterkategorien werden folgende Begriffe angeboten. Manche Filter benötigen ein Muster, nachdem gesucht werden soll. Wird kein Muster gesetzt, werden alle Gateways angezeigt.

Kategorie	Beschreibung	Muster
alle anzeigen	Zeigt alle verfügbaren Gateways an.	wird nicht benötigt
Name	Sucht nach Gateways, deren Namen auf das Muster passen (Gateway-Name, nicht Hostname). Das Muster muss nicht vollständig sein.	Das Muster kann der genaue Name sein oder ein Teil des Namens, wenn dieser nicht genau bekannt ist.
IP	Sucht nach Gateways, deren IP-Adresse auf das Muster passen. Das Muster muss nicht vollständig sein. Die Suche unterstützt auch Hostnamen.	Das Muster kann die genaue IP-Adresse sein oder ein Teil, wenn die Adresse nicht genau bekannt ist. z.B. 192.168.
Benutzer	Sucht nach Gateways, deren Benutzer (nicht Besitzer) auf das Muster passen. Das Muster muss nicht vollständig sein.	Das Muster kann der vollständige Name sein oder nur ein Teil des Namens, wenn dieser nicht genau bekannt ist.
Benutzergruppe	Sucht nach Gateways, deren eingetragene Benutzergruppen auf das Muster passen. Das Muster muss nicht vollständig sein.	Das Muster kann der vollständige Gruppenname sein oder nur ein Teil des Namens, wenn dieser nicht genau bekannt ist.

Muster werden auch immer als Teilmuster verstanden. Auch Groß- und Kleinschreibung werden nicht unterschieden. Z. B. findet das Muster `office` die Einträge `office`, `Office`, `home-office`, `office-max`, `officer`, `policeofficer` usw.



Abb. 45 Filter der Gateway-Liste

6.7 Benutzer und Benutzergruppen

Sie können für das Operation Center Benutzer anlegen, die Sie in Benutzergruppen organisieren können. Für Benutzer können eingeschränkte Benutzerrechte oder Administratorrechte vergeben werden. Nur Nutzer mit Administratorrechten können alle Funktionen des Operation Center nutzen. Der Administrator kann den Nutzern Lese- oder Lese- und Schreibrechte für einzelne Appliances im Menü ***UTM/VPN Gateways*** zuteilen oder verwehren.
Konten für Benutzer können Sie unter dem Punkt Benutzer anlegen und editieren. Benutzergruppen werden unter dem Punkt Benutzergruppen angelegt und verwaltet.
Die Zugriffsrechte von Benutzergruppen und deren Mitgliedern können unterschiedlich sein. Die Rechte des einzelnen Nutzers sind dann hochwertiger als die Rechte der Gruppe.

Beispiel: Der Gruppe Mitarbeiter ist nur Leserecht gewährt. Der Benutzer A ist Mitglied der Gruppe Mitarbeiter. Ihm sind in der Benutzerverwaltung Lese- und Schreibrechte zugewilligt. Somit kann er lesend und schreibend auf die Appliances zugreifen.

Hinweis: Ein neu angelegter Benutzer gehört keiner Gruppe an und sein Zugriffsrecht steht auf ***Verweigern***.



Abb. 46 Benutzerliste

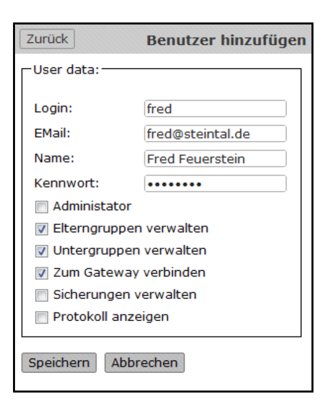


Abb. 47 Benutzer hinzufügen

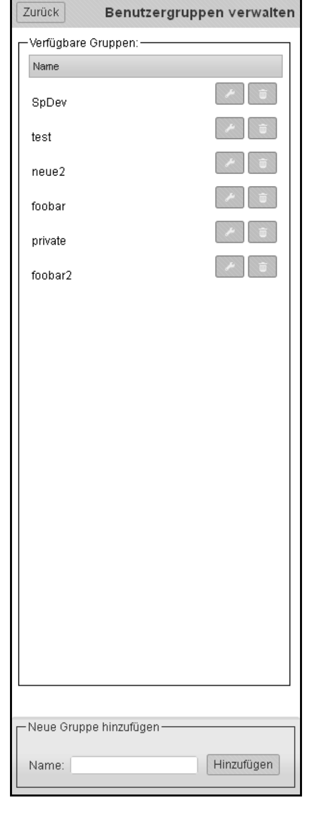


Abb. 48 Benutzergruppenliste

6.7.1 Neue Benutzer anlegen

- Um neue Benutzer anzulegen, nutzen Sie den Button ***Hinzufügen*** im Fenster ***Benutzer***.
  Es öffnet sich das Fenster ***Benutzer hinzufügen***.
- Geben Sie im Feld ***Login*** den Namen an, den der Benutzer für den Login nutzen soll.
- Im Feld ***E–Mail*** geben Sie eine E-Mail-Adresse des Benutzers an. An diese E-Mail-Adresse können dem Nutzer automatisch generierte Berichte oder Nachrichten über Ereignisse und Alarme gesendet werden.
- Im Feld ***Namen*** tragen sie den Namen des Nutzers ein.
- Im Feld ***Kennwort*** tragen Sie das Kennwort für den Login ein.
- Als ***Benutzerrechte*** stehen Ihnen folgende zur Auswahl:
  - ***Administrator:*** Der Benutzer hat alle Rechte zur Verfügung.
  - ***Elterngruppe verwalten:*** Der Benutzer darf die Hauptgruppen der Gateway Gruppen verwalten.
  - ***Untergruppe verwalten:*** Der Benutzer darf die Untergruppen der Gateway Gruppen verwalten.
  - ***Zum Gateway verbinden:*** Der Benutzer darf sich per SSH zu den für Ihn sichtbaren Gateways verbinden.
  - ***Sicherung verwalten:*** Der Benutzer darf Sicherungen der Firewall exportieren und zurückspielen.
  - ***Protokoll anzeigen:*** Dem Benutzer wird das Protokoll des Operation Centers angezeigt.
- Klicken Sie auf ***Speichern***, um die Daten abzuspeichern.

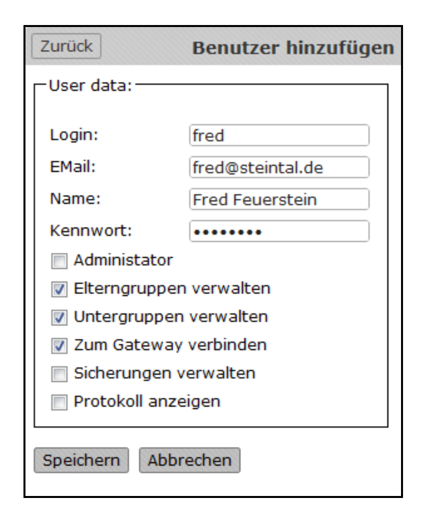


Abb. 49 Benutzer hinzufügen

6.7.2 Benutzerdaten bearbeiten

Wenn Sie in der Benutzerliste auf das Icon mit dem Werkzeugschlüsselsymbol klicken, öffnet sich ein Bearbeitungsdialog.

Der Dialog zeigt mehr Einstellungen, als Sie im ***Benutzer hinzufügen*** Dialog angeboten bekommen.

Sie können hier die E-Mail-Adresse, den Namen und die Benutzerrechte ändern.

Mit der Schaltfläche ***Zurücksetzen*** im Bereich ***Kennwort zurücksetzen***, können Sie ein neues Kennwort für den Benutzer festlegen,

Im Bereich ***Gruppen*** können Sie die Benutzergruppen-mitgliedschaft prüfen, weitere hinzufügen und bestehende entfernen.

Im Bereich ***UTM/VPN Gateways*** wird Ihnen angezeigt, welche Gateways dem Benutzer im Rahmen einer Gruppe oder direkt zugewiesen sind und ob er der Besitzer ist. Um dies einsehen zu können, müssen Sie aber mindestens Leserechte für die eingetragenen Gateways haben. Dieser Bereich ist nur zur Ansicht. Es können keine Änderungen vorgenommen werden.

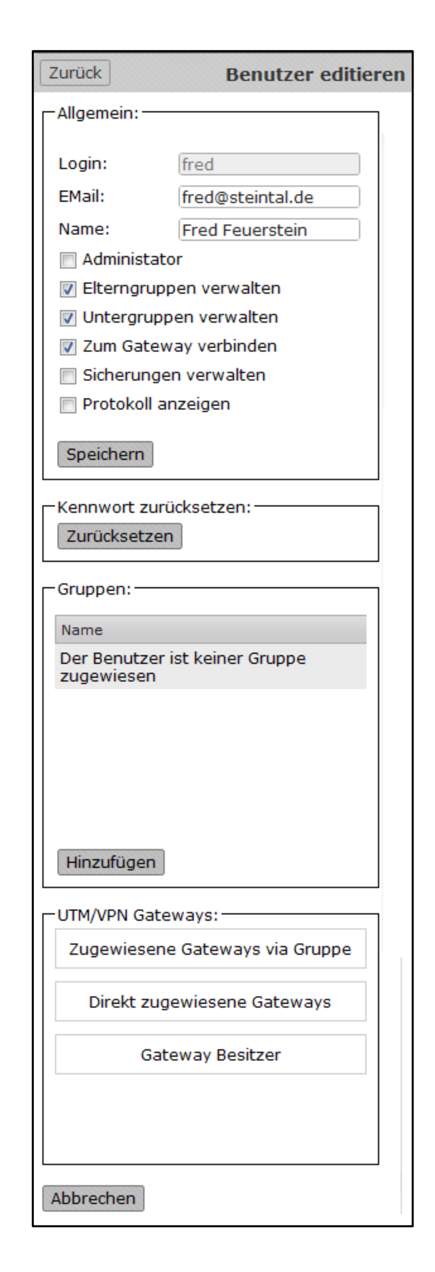


Abb. 50 Benutzereinstellungen bearbeiten

6.7.3 Nachrichten an Benutzer senden

Unter dem Menüpunkt Benutzer wird eine Liste aller eingetragenen Benutzer angezeigt.
Am jedem Zeilenende befindet sich ein ***Briefumschlagsymbol***.
Ein Benutzer mit eingeschränkten Rechten wird nur das ***Briefumschlagsymbol*** angezeigt.
Benutzer mit Administratorrechten werden zusätzlich die Buttons ***Bearbeiten*** und ***Löschen*** angezeigt.

Mit dem Button ***Nachricht an alle senden*** unter der Liste können Sie eine Nachricht verfassen, die an alle eingetragenen Benutzer versendet wird.

- Wenn Sie den Button am Zeilenende betätigen, öffnet sich die Ansicht ***Nachricht senden***.
- Geben Sie im Feld ***Betreff*** einen Betreff für die Nachricht ein.
- Geben Sie im ***Textfeld*** darunter Ihre Nachricht an.
- Klicken Sie zum ***Absenden*** auf Senden.
- Die Nachricht wird in der Übersicht im Abschnitt ***Nachrichten*** angezeigt. Beim nächsten Login wird dem Benutzer eine Meldung über den Erhalt einer neuen Nachricht angezeigt.



Abb. 51 Liste aller eingetragenen Benutzer

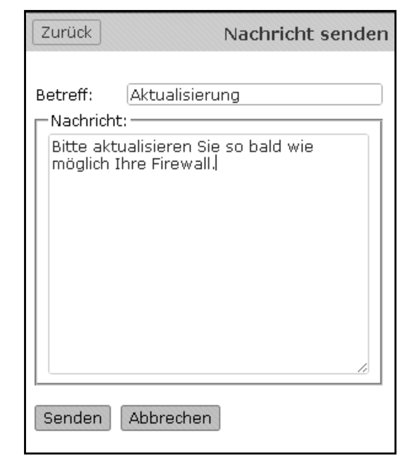


Abb. 52 Verfassen einer Nachricht

6.8 Images

Die Schaltfläche ***Images*** im Menü ***Extras*** öffnet die Securepoint Image Verwaltung. Die Verwaltung bietet ihnen die Möglichkeit, Securepoint Appliance Images vom Securepoint Download Server herunterzuladen. Die Images werden auf dem System gespeichert, auf dem der Datenprovider installiert ist.
Von diesen heruntergeladenen Images können sie Installationsabbilder für Securepoint Systeme oder Terra Systeme erstellen und direkt mit dem Securepoint Imaging Tool auf eine USB- Speicherstick übertragen.
Zusätzlich haben Sie die Möglichkeit Konfigurationen anzulegen und an die Images zu binden. Dadurch können Sie neben dem Installationsimage eine Startkonfiguration auf einem USB- Speicherstick speichern.
Sie können die Konfiguration auch aus einer Sicherung einer eingetragenen Aplliance erstellen.

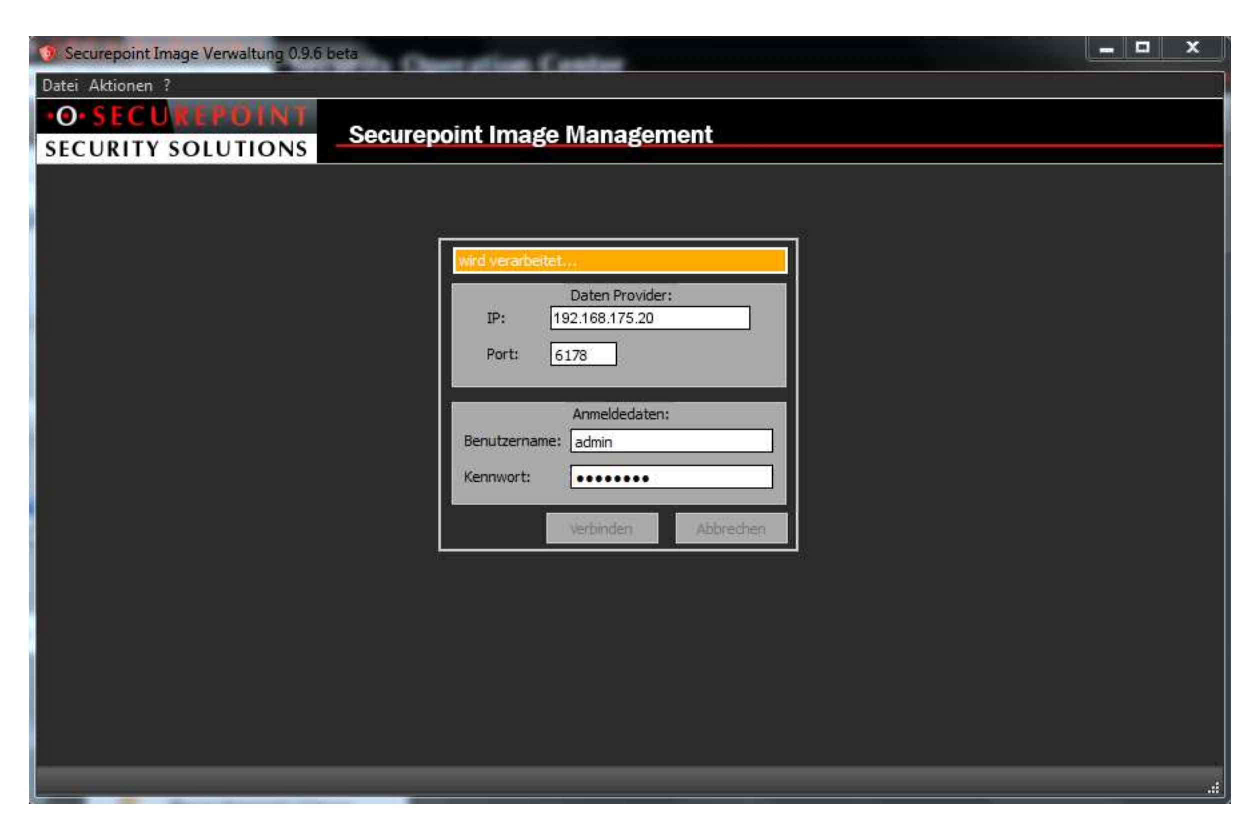


Abb. 53 Verbindung zum Datenprovider wird automatisch hergestellt.

6.8.1 Registerkarte Images

Bei Start der Securepoint Image Verwaltung öffnet sich die Registerkarte ***Images***. Hier werden Images angezeigt, an denen eine Konfiguration gebunden ist. Diese Konfiguration kann aus einer Sicherung stammen oder extra erstellt sein.

Es stehen Ihnen die Aktionen ***Löschen*** und ***Erstellen als…*** zur Verfügung. Die Schaltfläche ***Erstellen als…***, stellt Ihnen die Erstellung des Image als Securepoint-System oder als Terra-System zur Auswahl.

- Durch Klicken auf den Button ***Erstellen als…*** öffnet sich ein Dropdownmenü mit den Einträgen ***Securepoint*** und ***Terra***.
- Wählen Sie durch Klicken auf den entsprechenden Eintrag ein System aus.
- Es öffnet sich das ***Securepoint Imaging Tool***. Welches Ihnen ermöglicht, das gewählte Image auf ein USB Speichermedium zu kopieren.

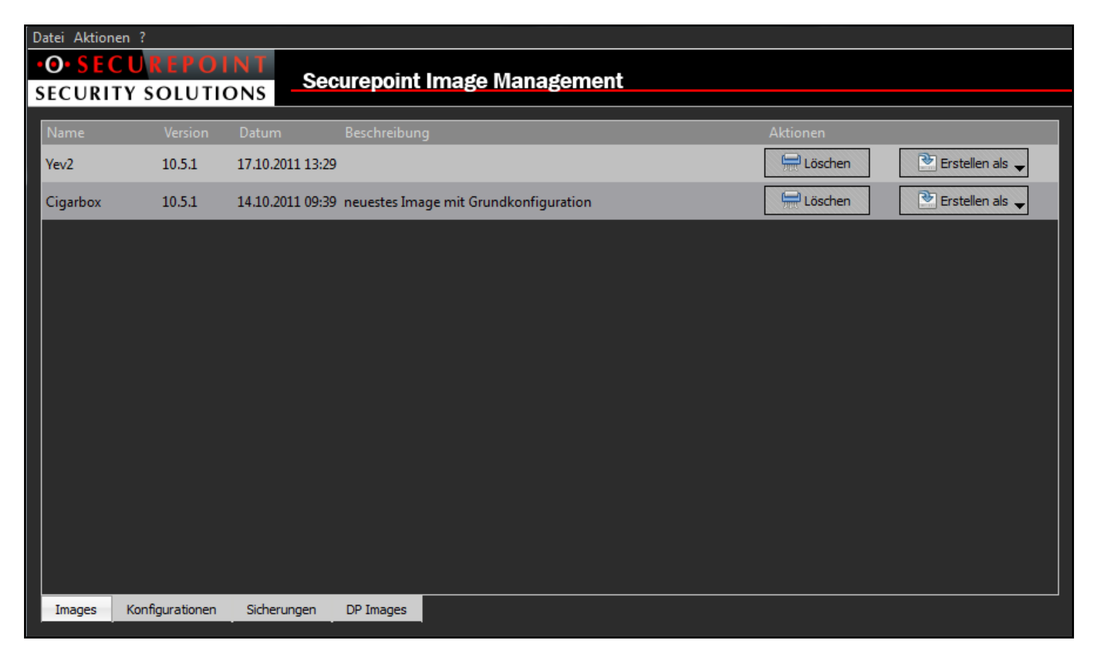


Abb. 54 Registerkarte Image

6.8.2 Registerkarte Konfigurationen

Auf der Registerkarte ***Konfiguration*** werden Ihnen Konfigurationen angezeigt, die mit der Image Verwaltung erstellt wurden.
Die Aktion ***Zuweisen*** ermöglicht Ihnen die Konfiguration an ein Image zu binden, welches auf dem Datenprovider verfügbar ist. Die erstellte Kombination aus Image und Konfiguration wird dann auf der Registerkarte ***Images*** gelistet.

- Klicken Sie auf ***Zuweisen***. Es öffnet sich ein neuer Dialog, in dem alle verfügbaren Versionen angezeigt werden.
- Geben Sie für die Zusammenstellung in dem Feld ***Name*** einen Titel ein.
  Optional können Sie auch einen ***Beschreibung*** im gleichnamigen Feld eingeben.
- Klicken Sie dann bei der gewünschten Version auf ***Zuweisen***.

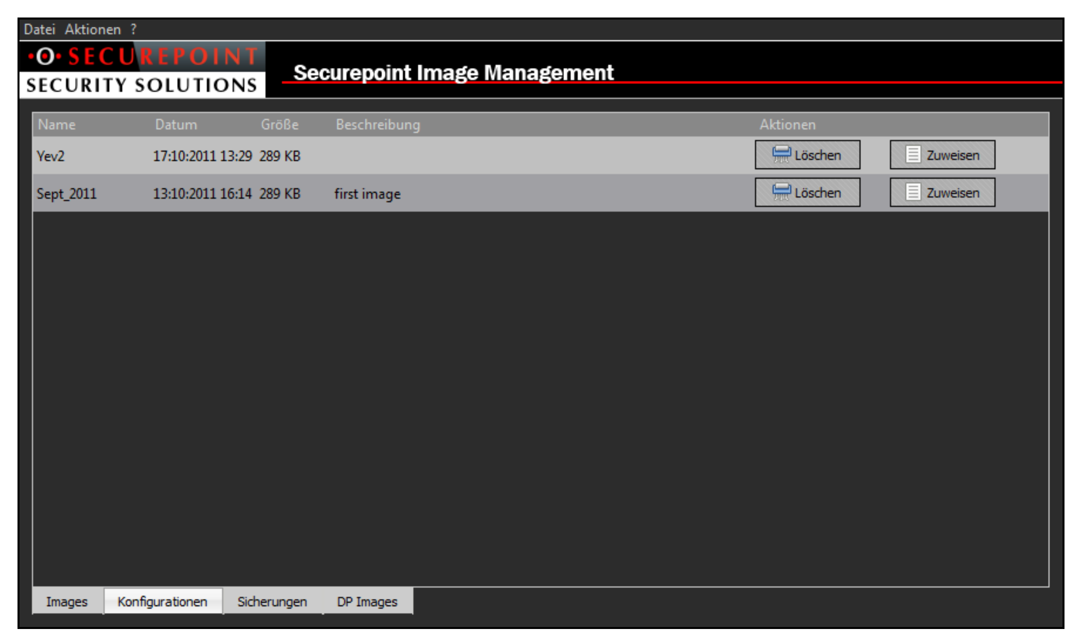


Abb. 55 Registerkarte Konfigurationen

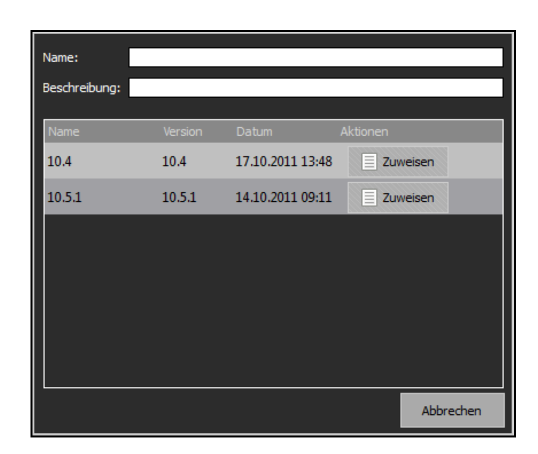


Abb. 56 Dialog zur Auswahl der Version

6.8.3 Registerkarte Sicherungen

Auf dieser Registerkarte werden alle verfügbaren Sicherungen angezeigt, die durch das SOC angelegt wurden. Auch diese können als Konfiguration an ein Image gebunden werden und werden dann als Kombination aus Image und Konfiguration auf der Registerkarte ***Images*** gelistet.

- Klicken Sie in der Zeile der gewünschten Sicherung auf ***Zuweisen***.
  Es öffnet sich ein neuer Dialog, der alle verfügbaren Versionen auflistet.
- Geben Sie für das neue Image einen Titel im Feld ***Name*** ein.
- Optional können sie eine ***Beschreibung*** im gleichnamigen Feld eintragen.
- Klicken Sie dann in der Zeile der gewünschten Version auf ***Zuweisen***.
  Das Verwaltungsprogramm erstellt ein Image und listet es auf der Registerkarte ***Images*** auf.

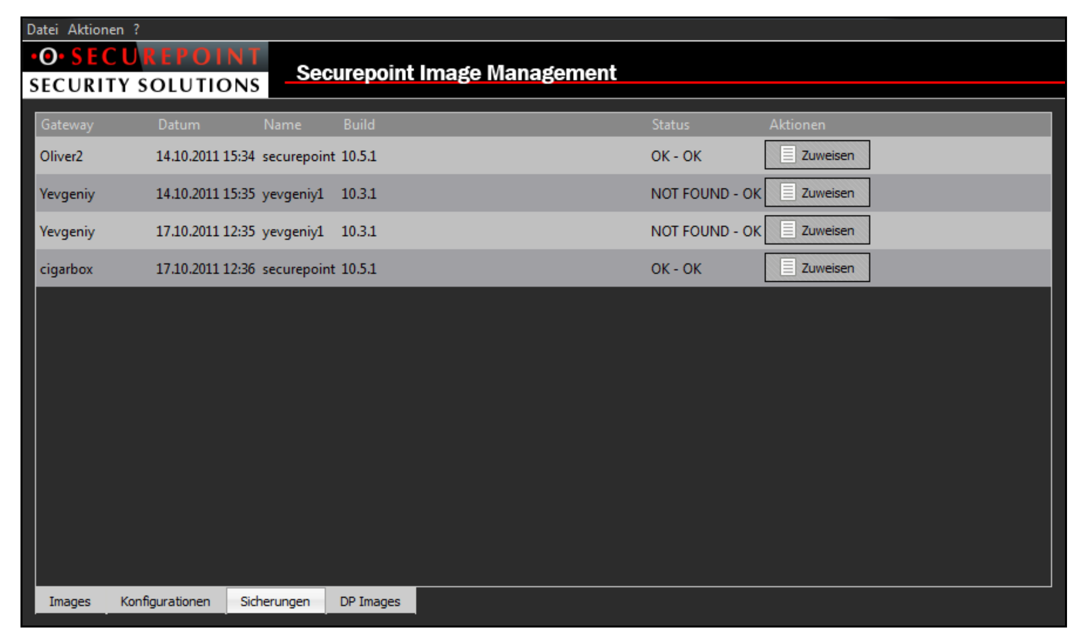


Abb. 57 Registerkarte Sicherungen

6.8.4 Registerkarte DP Images

DP Images steht für Datenprovider Images. Hier werden alle Versionen der Appliances Betriebssysteme aufgelistet, die auf dem System, auf dem auch der Datenprovider betrieben wird, gespeichert sind und somit für die Image Verwaltung zur Verfügung stehen.

- Wenn Sie weitere Versionen vom Securepoint Download Server herunterladen möchten, benutzen Sie die Schaltfläche ***Neues Image hinzufügen***, welche sich direkt über der Registerkartenleiste befindet.
- Es öffnet sich ein Dialog, der alle Appliances Betriebssysteme, die auf dem Securepoint Download Server verfügbar sind, auflistet. Klicken Sie in der Zeile der gewünschten Version auf ***Herunterladen***. Anschließend wird die Version auf dem Datenprovider-System gespeichert.

Es stehen Ihnen die Aktionen ***Löschen*** und ***Erstellen als…*** zur Verfügung. Die Schaltfläche ***Erstellen als…***, stellt Ihnen die Erstellung des Image als Securepoint-System oder als Terra-System zur Auswahl.

- Durch Klicken auf den Button ***Erstellen als…*** öffnet sich ein Dropdownmenü mit den Einträgen ***Securepoint*** und ***Terra***.
- Wählen Sie durch Klicken auf den entsprechenden Eintrag ein System aus.
- Es öffnet sich das ***Securepoint Imaging Tool***. Welches Ihnen ermöglicht, das gewählte Image auf ein USB Speichermedium zu kopieren.

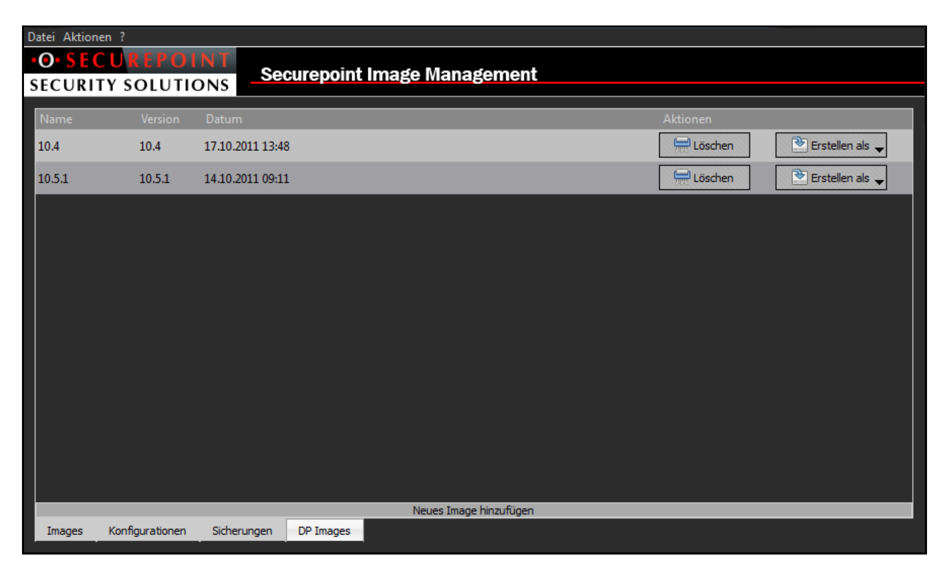


Abb. 58 Registerkarte DP Images

Abb. 59 Images auf dem Download Server

6.8.5 Erstellen einer Neuen Konfiguration

Die Securepoint Image Verwaltung stellt Ihnen einen Assistenten zur Verfügung, mit dem Sie eine Konfiguration erstellen können. Der Assistent leitet Sie durch die einzelnen Schritte und speichert anschließend die Konfiguration auf dem Datenprovider-System. Die so erstellten Konfigurationen werden in der Image Verwaltung auf der Registerkarte Konfigurationen aufgelistet.

- Klicken Sie in der Menüleistet der Securepoint Image Verwaltung auf den Menüpunkt ***Aktionen*** und wählen Sie im Dropdownmenü den Eintrag ***Assistent öffnen***.

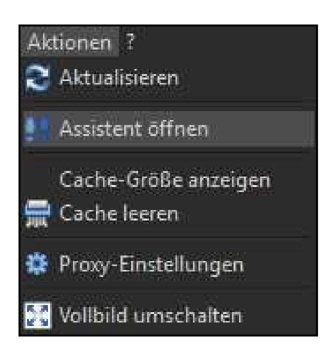


Abb. 60 Menü Aktionen

- Im gestarteten Assistenten werden Sie aufgefordert einen ***Namen*** für die neue Konfiguration anzugeben.
- Optional können Sie im Feld ***Beschreibung*** noch eine nähere Beschreibung für die Konfiguration angeben.
- Klicken Sie nach der Eingabe auf ***Next***.

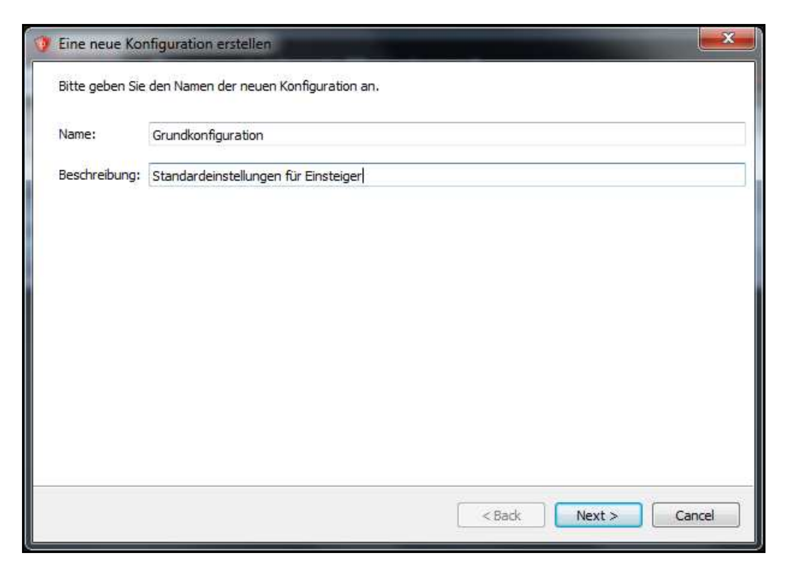


Abb. 61 Schritt 1 - Name eingeben

- Im zweiten Schritt wird Ihnen die ***Lizenzvereinbarung*** angezeigt. Lesen Sie diese sogfältig durch. Wenn Sie mit den Bedingungen einverstanden sind, klicken Sie auf ***Next***.
- Klicken Sie auf ***Cancel***, wenn Sie mit den Bedingungen nicht einverstanden sind. Der Assistent wird dann beendet.

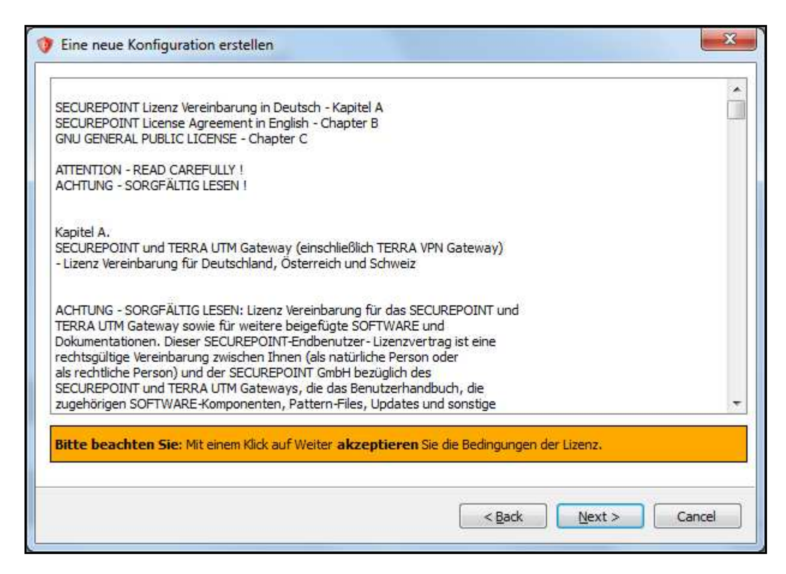


Abb. 62 Schritt 2 - Anzeige der Lizenzbedingungen

- Geben Sie im nächsten Schritt die ***interne IP Adresse*** der Appliance ein.
  Dies ist die Adresse über die die Appliance administriert wird und die Gateway Adresse des internen Netzwerkes.
- Die ***Netzwerkmaske*** unterteilt die IP Adresse in Netzwerkteil und Geräteteil. Vereinfacht kann gesagt werden, dass sie entscheidet, wie viele IP-Adressen im Subnetz verfügbar sind.

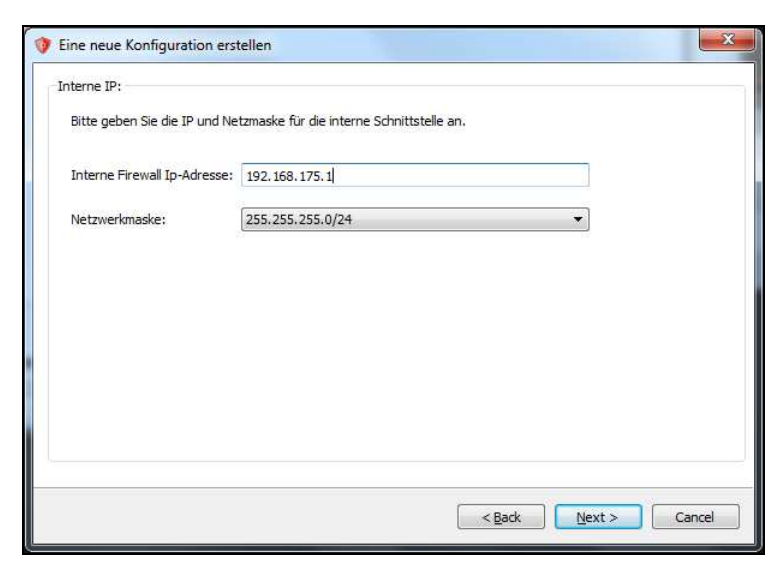


Abb. 63 Schritt 3 - Eingabe der internen IP Adresse und der Netzwerkmaske

Der nächste Schritt fragt die Anschlussart der externen Schnittstelle ab.

- Wählen Sie zwischen ***DSL-PPPoE***, ***Ethernet mit statischer IP-Adresse*** oder ***Kabelmodem mit DHCP-Client***.
- Klicken Sie auf ***Next***.

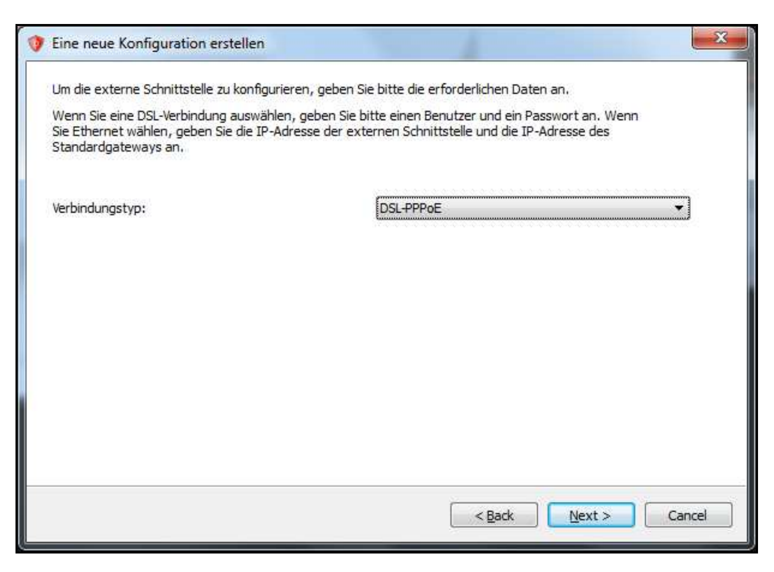


Abb. 64 Schritt 4 - Anschlusstyp der externen Schnittstelle

In Abhängigkeit des Anschlusstyps variiert der nächste Dialog.

Wenn die externe Schnittstelle mit einem DSL Anschluss verbunden wird, werden die Benutzerdaten für den Internet Service Provider benötigt.

- Wählen Sie aus dem Dropdownmenü ***Provider*** Ihren DSL Anbieter aus.
- In Abhängigkeit des Anbieters variieren die weiteren Felder. Geben Sie geforderten Angaben an. Diese müssen Ihnen vom Anschlussanbieter bei Anschlussübergabe angegeben worden sein.
- Klicken Sie auf ***Next***.

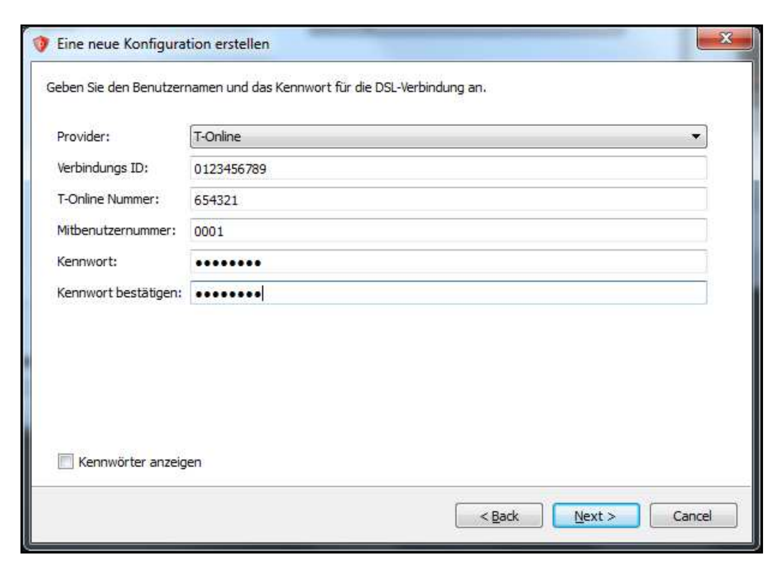


Abb. 65 Schritt 5a - Benutzername und Kennwort für den DSL Anschluss

- Wenn Sie die Appliance in einem Ethernet Netzwerk mit statischer IP-Adresse angeschlossen haben, geben Sie die IP-Adresse für die externe Schnittstelle im Feld ***Externe Firewall-IP-Adresse*** an.
- Wählen Sie aus dem Dropdownmenü ***Netzwerkmaske*** die passende Maske.
- Geben Sie im Feld ***Gateway***, die IP-Adresse des Gateways an.
- Klicken Sie auf ***Next***.

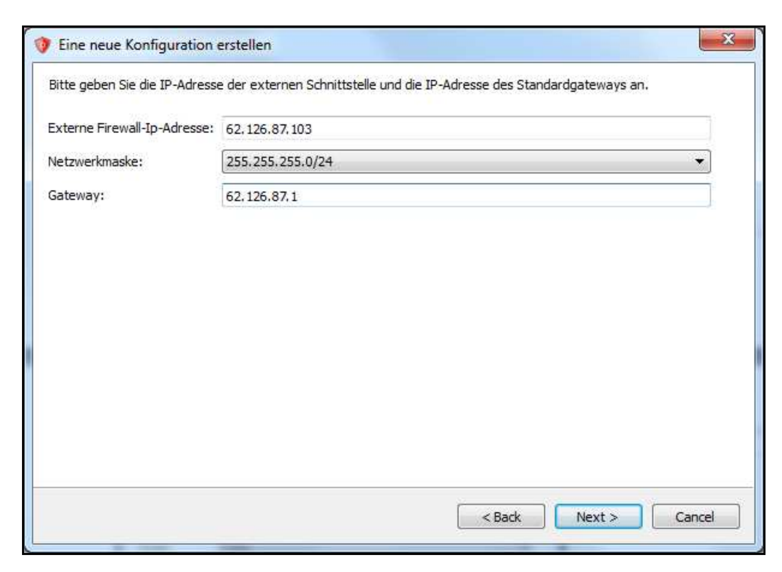


Abb. 66 Schritt 5b - Anschluss mit statischer IP-Adresse

- Wen Sie eine DMZ (Demilitarisierte Zone) einrichten möchten, geben Sie die IP-Adresse für die dritte Schnittstelle im Feld ***DMZ IP-Adresse*** an.
- Wählen Sie im Dropdownmenü ***Netzwerkmaske*** die passende Maske.
- Klicken Sie auf ***Next***.
- Möchten Sie ***keine*** DZ anlegen, dann machen Sie keine Eingaben und klicken gleich auf ***Next***.

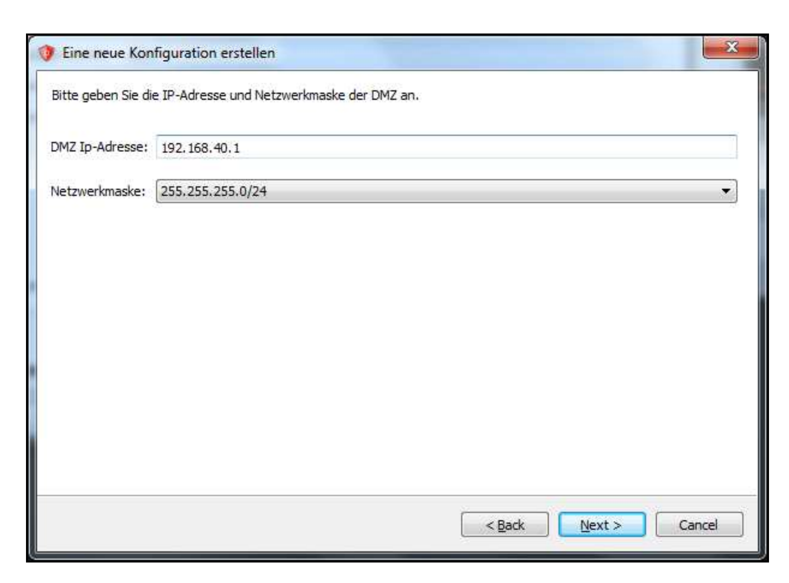


Abb. 67 Schritt 6 - IP-Adresse für die DMZ angeben (optional)

Im nächsten Schritt legen Sie ein Kennwort für den Standardbenutzer fest.

- Der ***Benutzername*** des Standardbenutzers ist nicht änderbar und heißt ***admin***.
- Geben Sie unter ***Neues Kennwort*** ein neues Kennwort ein.
- Wiederholen Sie die Eingabe im Feld ***Kennwort bestätigen***.
- Die Eingabe ist nicht lesbar. Wenn Sie die Eingaben lesen möchten aktivieren Sie die Checkbox ***Kennwörter anzeigen***.
- Wenn Sie auf der Aplliance einen Superuser Account mit dem Namen root anlegen möchten, aktivieren Sie die Checkbox ***Root-Benutzer mit diesem Kennwort anlegen***.
- Klicken Sie ***Next***.

Hinweis: Ein sicheres Kennwort ist mindestens 8 Zeichen lang und besteht aus Klein- und Großbuchstaben, Ziffern und Sonderzeichen.

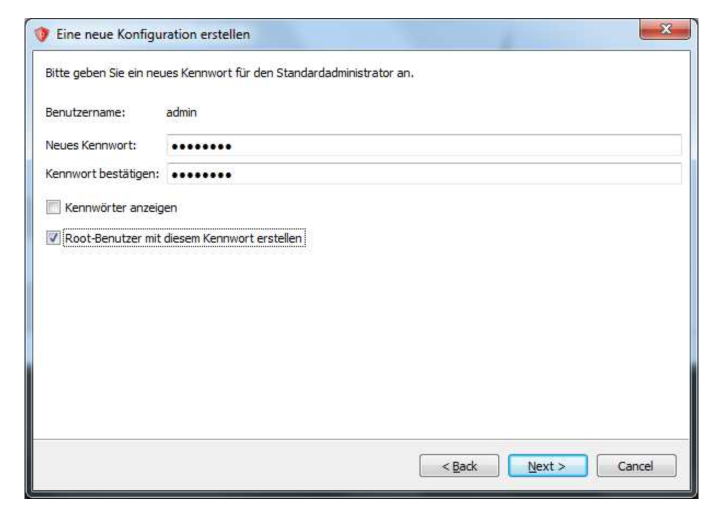


Abb. 68 Schritt 7 - Kennwort fürd den Standardbenutzer festlegen

- Im letzten Schritt wird Ihnen eine Zusammenfassung angezeigt.
- Klicken Sie auf ***Finish***, um den Assistenten zu schließen und die Konfiguration zu speichern.
- Die Konfiguration wird auf der Registerkarte ***Konfigurationen*** mit aufgelistet.

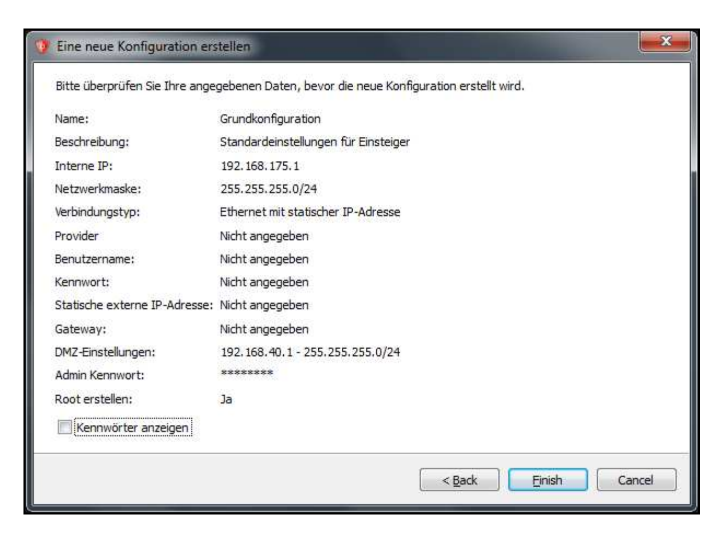


Abb. 69 Zusammenfassung der erhobenen Daten

7 Operation Center

In diesem Abschnitt befinden sich Funktionen und Einstellungen, die das Operation Center betreffen.



Abb. 70 Menü Operation Center

Schaltfläche	Beschreibung
Dienststatus	Zeigt eine Tabelle an, wann die Dienste Sicherung, Überwachung und Aufgaben den Datenprovider zum letzten Mal abgefragt haben. Außerdem können Details der Dienste angezeigt werden. Z.B. CPU Auslastung und Speichernutzung.
Wer ist online	Zeigt eine Liste an, welche Nutzer momentan mit dem Operation Center auf den gleichen Datenprovider zugreifen.
Vollbild umschalten	Schaltet das Security Operation Center in den Vollbildmodus. Um zum Fenstermodus zurückzukehren, muss die Schaltfläche nochmals betätigt werden. Oder benutzen Sie F11.
Einstellungen	Öffnet einen Bereich, in dem grundlegende Einstellungen des Operation Centers getätigt werden.
Protokoll Einstellungen	Einstellung der Vorhaltezeit für Protokolleinträge.
Sicherungsdienst	Öffnet die Einstellung des Sicherungsdienstes. Dieser legt ein Backup der Konfigurationen aller eingestellten Appliances an.
Datenquelle	Der Data Provider ist ein Dienst, der auf die Datenbank zugreift und die angeforderten Daten auf Benutzerrechte überprüft. Das SOC greift immer über den Data Provider auf die Datenbank zu, auch bei einer lokalen Installation.
Überwachung	Öffnet die Einstellungen des Monitorings (siehe Kapitel 4.2).
Anwendung beenden	Beendet das Security Operation Center.

7.1 Dienststatus

Unter dem Punkt Dienststatus wird der letzte Zugriffszeitpunkt der Dienste auf die Datenbank angezeigt. So kann überprüft werden ob die Dienste noch ordnungsgemäß ausgeführt werden. Durch den Button ***Aktualisieren*** wird die Ansicht neu geladen.



Abb. 71 Letzte Abfrage der Datenbank

In der zweiten Liste wird angezeigt, auf welcher IP-Adresse die Dienste laufen.

Wenn Sie auf das Icon ***erweitern*** anklicken, öffnet sich eine neue Ansicht mit Detaildaten zum Dienststatus.
Im Bereich ***Allgemein*** wird die durchschnittliche CPU- und Speicherauslastung angezeigt.

Feld	**Beschreibung**
Läufe	Anzahl der durchgeführten Läufe. Maximal 400 Läufe werden aufgezeichnet, ältere werden überschrieben.
∅ CPU	Durchschnittliche CPU Beanspruchung.
∅ Working	Durchschnittliche Speichernutzung. Auch Speicherbenutzung von verwendeten DLLs wird mit berechnet.
∅ Private	Durchschnittliche Speichernutzung des Dienstes.
CPU maximal	Maximale CPU Beanspruchung.
Working maximal	Maximale Speichernutzung mit verwendeten DLLs und Anwendungen.
Private maximal	Maximale Speichernutzung des Dienstes.
Letzte Aktion	Letzte Aktion des Dienstes beim Aufrufen der Details.
Letzte Aktualisierung	Letzte Aktualisierung der Detaildaten.

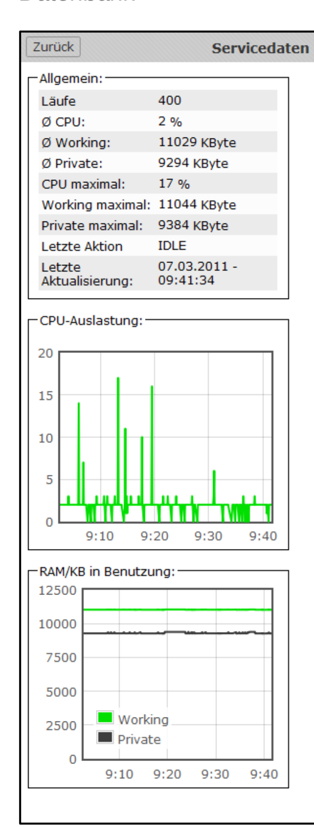


Abb. 72 Hardware-Auslastung durch einen Dienst

Der Bereich ***CPU-Auslastung*** zeigt die Prozessorlast, die durch den Dienst verursacht wird. Die Last wird im Graph gegen die Zeit aufgetragen.
Im Bereich ***RAM/KB in Benutzung*** wird die Speichernutzung des Dienstes gegen die Zeit aufgetragen. ***Private*** ist die Last, die vom Dienst allein verursacht wird. Der Wert ***Working*** beinhaltet die Speichernutzung des Dienstes und die benutzen Anwendungen und DLLs des Dienstes.

7.2 Wer ist online

Unter dem Menüpunkt ***Wer ist online*** können Sie einsehen, welche Benutzer sich zu diesem Zeitpunkt am Datenprovider angemeldet haben.

Die Liste der angemeldeten Benutzer beinhaltet den Nutzernamen und die IP-Adresse des Clientrechners der angemeldeten Benutzer. Außerdem wird noch der Zeitpunkt des letzten Suchlaufs angezeigt.

Der Button am Ende der Nutzerzeile öffnet einen Chat Dialog zu dem jeweiligen Benutzer.

Mit dem Button ***An alle senden*** am Ende der Liste können Sie eine Chat Nachricht an alle angemeldeten Benutzer gleichzeitig senden.

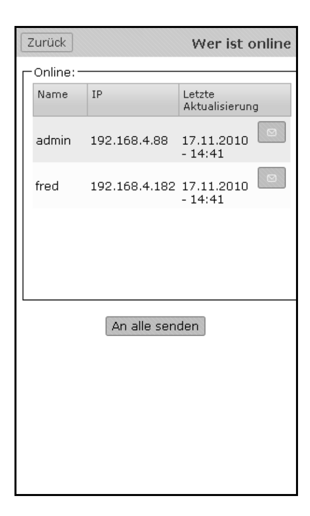


Abb. 73 Anzeige der angemeldeten Benutzer

7.2.1 Online Chat

- Um eine Chat-Sitzung zu beginnen, klicken sie auf den Button mit dem ***Briefumschlagsymbol***. Es öffnet sich ein Chat-Dialog.
- Geben Sie den gewünschten Text im Dialog ein.
- Betätigen Sie die ***Eingabetaste***, um die Nachricht abzusenden.
- Ihre Nachricht wird nun im oberen Bereich des Dialogs angezeigt.
  Beim anderen Benutzer öffnet sich der Chat-Dialog im Vordergrund. Antworten des Benutzers werden direkt im oberen Bereich angezeigt.
  Zur Unterscheidung der Meldungen werden Ihre Meldungen, Ihr Benutzername und die Zeit der Versendung in ***blauer Schrift*** vorangestellt. In ***roter Schrift*** werden den Meldungen des anderen Nutzers der Benutzername und die Zeit des Empfangs vorangestellt.

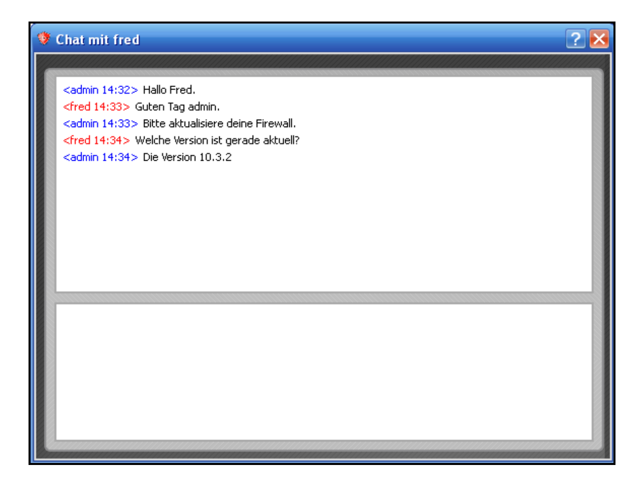


Abb. 74 Chat-Dialog

7.3 Einstellungen des Operation Centers

In diesem Bereich können grundlegende Optionen für das Operation Center festlegen. Darunter fallen z. B. Speicherorte, Ansicht/Layout und Proxy-Einstellungen.

7.3.1 Registerkarte Allgemein

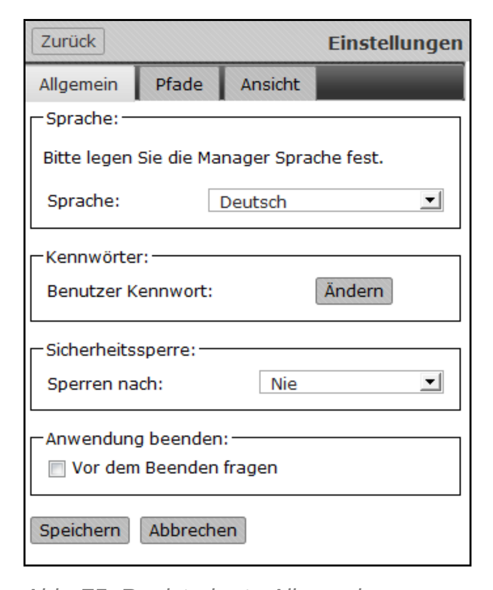


Abb. 75 Registerkarte Allgemein

Bezeichnung	Beschreibung
Sprache	Legt die Sprache des Operation Centers fest. Eine Änderung wird erst bei einem Neustart übernommen.
Kennwörter	Ändern des Kennwortes des aktuellen Benutzers.
Sicherheitssperre	Wird das SOC in der definierten Zeitspanne nicht benutzt, wird es gesperrt. Zum Entsperren müssen Sie Ihr Kennwort eingeben.
Anwendung beenden	Festlegen, ob eine Sicherheitsabfrage beim Beenden des Operation Centers angezeigt wird.

7.3.2 Registerkarte Pfade

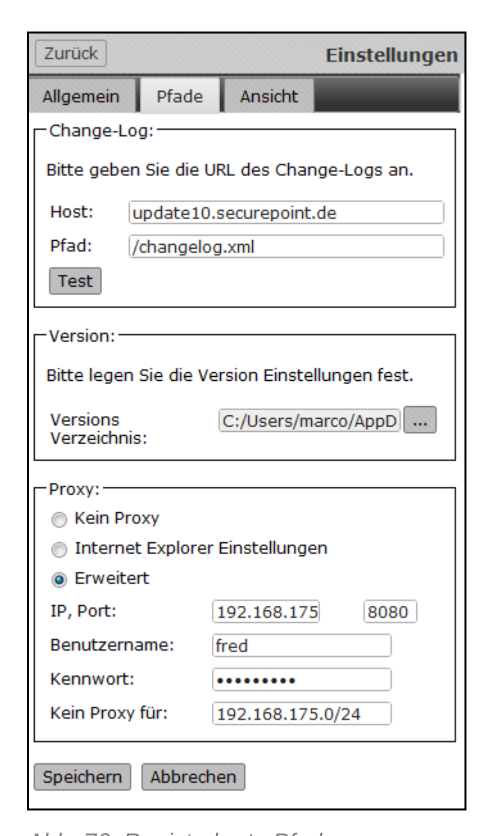


Abb. 76 Registerkarte Pfade

Bezeichnung	Beschreibung
Change-Log	Im Change-Log werden die Änderungen von Version zu Version der Firewall-Software aufgezeichnet. Geben Sie die URL und den Dateinamen des Change-Logs an. Diese Angaben sind nötig, um die Funktion im Webinterface aufzurufen und für das Monitoring.
Version	Zum Festlegen des Verzeichnisses, in das neue Versionen abgelegt werden.
Proxy	Einstellungen für die Benutzung eines Proxys. Speicherung von Anmeldedaten und Angabe von Proxy Ausnahmen. **Hinweis:** NTLM Authentifizierung wird nicht unterstützt.

7.3.3 Registerkarte Ansicht

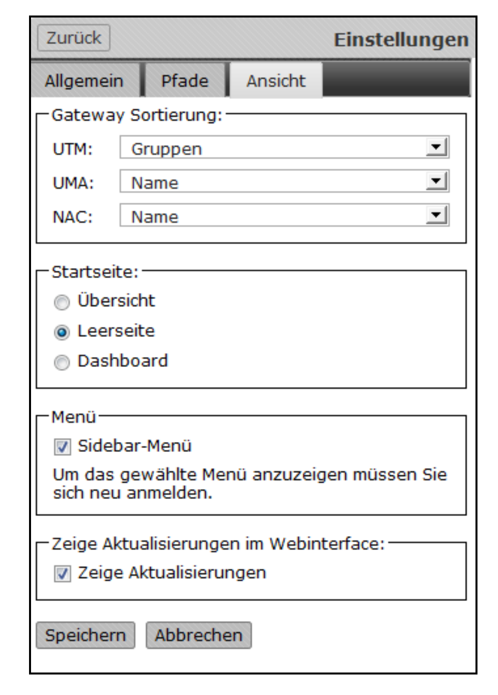


Abb. 77 Registerkarte Ansicht

Bezeichnung	Beschreibung
Gateway Sortierung	Voreinstellung der Sortierung der verschiedenen Gateway Kategorien beim Start des Gateway Centers.
Startseite	Wählen Sie den Inhalt des rechten Fensters beim Start. Möglichkeiten: Übersicht – Message Board Leerseite – kein Inhalt Dashboard – Monitoring in Boxenansicht
Menü	Wechseln auf das Sidebar Menü. Die Änderung wird erst bei einer Neuanmeldung angewendet. Benutzen Sie zu Neuanmeldung die Taste F5.
Zeige Aktualisierungen	Ist diese Option gesetzt, wird bei Verbindung mit einer Appliance eine Information angezeigt, wenn eine neue Version

	der Firewall-Software vorliegt.

7.4 Sicherungsdienst

Der ***Sicherungsdienst*** stellt eine Backup Funktion für die Konfigurationen aller eingetragenen Appliances zu Verfügung.
Die Sicherungen werden in der Datenbank abgelegt. Es werden pro Appliance zehn Sicherungen gespeichert. Wird eine weitere Sicherung angelegt, wird die älteste Sicherung aus der Datenbank gelöscht.
Die gespeicherten Konfigurationen können Sie im Bereich ***UTM/VPN Gateways*** wieder zurückspielen.

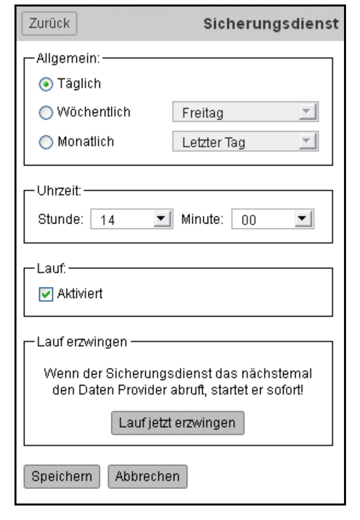


Abb. 78 Backup Einstellungen

Bezeichnung	Beschreibung
Allgemein	Hier wird der Turnus der Sicherung angegeben. Sie können die Sicherung täglich, wöchentlich oder monatlich anlegen.
Uhrzeit	Stellen Sie die Uhrzeit ein, zu der die Sicherung angelegt werden soll.
Lauf	Nur wenn die Option Aktiviert gesetzt ist, werden Sicherungen angelegt.
Lauf erzwingen	Mit dieser Schaltfläche wird sofort eine Sicherung aller Appliances durchgeführt.

7.5 Datenquelle

Unter diesem Punkt können Sie die IP-Adresse des Data Providers angeben.
Der Data Provider ist ein Dienst, der die Verbindung zur Datenbank herstellt, in der alle Monitoringdaten, Sicherungen, Aufgaben und Protokolldaten gespeichert sind. Die Verbindung zur Datenbank ist nicht nur nötig, um bestehende Daten in das Operation Center zu laden, sondern auch, um neue Daten in die Datenbank zu schreiben. Des Weiteren erstellt der Data Provider Dienst eine Protokollierung der durchgeführten Bedienungsschritte aller Benutzer. Die Protokollierung umfasst nur die Bedienung des Operation Centers und nicht Einstellungen, die über die SSH-Verbindung an den Appliances durchgeführt werden. So kann nachverfolgt werden, welche Aktionen die Benutzer im Operation Center durchgeführt haben.
Ohne eine Verbindung zu einem Data Provider wird das Operation Center nicht gestartet. Deshalb wird beim Start des Operation Centers überprüft, ob eine Verbindung zu einem Data Provider Dienst besteht.
Der Dienst kann auf dem lokalen Rechner installiert werden oder zentral auf einem Server. Wenn der Datenprovider zentral gehalten wird, kann von verschiedenen Rechnern auf die Datenbank zugegriffen werden.
Über das Installationssetup, kann man auswählen, welche Komponenten installiert werden sollen. Der Data Provider Dienst trägt den Namen Securepoint Data Provider. Dieser wird standardmäßig installiert und beim Systemstart ausgeführt. Der Dienst benutzt den Port 6178.

Wird der Data Provider Dienst auf einem Server gehalten, der rund um die Uhr in Betrieb ist, hat das den Vorteil, dass Monitoring Daten, Backups und Protokolldaten fortlaufend erstellt und gespeichert werden, auch wenn der lokale Rechner, auf dem das Operation Center installiert ist, ausgeschaltet ist. Außerdem werden auch Aktionen von anderen Security Operation Centern protokolliert. Ein weiterer Vorteil ist, dass auf diese Daten von allen Rechnern zugegriffen werden kann, soweit auf diesen das Security Operation Center installiert ist. Dies gilt nicht nur für das lokale Netzwerk, sondern auch für externe Mitarbeiter, die sich zum Beispiel über ein VPN mit dem Intranet verbinden.
Durch die Vergabe von Lese- und Schreibrechten, kann auch bei einem zentral gehaltenen Dienst gewährleistet werden, dass Benutzer nur Daten der Appliances einsehen können, für die sie Leserechte oder Lese- und Schreibrechte haben.

7.5.1 Datenquelle beim Start eingeben

- Beim Start des Security Operation Centers wird versucht, eine Verbindung zum lokalen Dienst Data Provider (IP-Adresse 127.0.0.1) aufzubauen.
  Wenn dieser Dienst nicht aktiv ist oder gar nicht installiert wurde, haben Sie die Möglichkeit, eine ***IP-Adresse*** eines Rechners einzutragen, auf dem der Dienst verfügbar ist.
- Klicken Sie auf ***Test***, um die Verbindung aufzubauen und auf den Dienst zu prüfen.
- Ist der Test erfolgreich, wird der Button ***Speichern*** aktiviert. Speichern Sie die IP-Adressen mit diesem.
- Erst jetzt können Sie sich mit den Anmeldedaten am Operation Center anmelden. Tragen Sie Ihren ***Benutzernamen*** und das ***Kennwort*** in die entsprechenden Felder ein und klicken Sie auf ***Anmeldung***.



Abb. 79 neue IP-Adresse eintragen



Abb. 80 Anmeldung am System

7.5.2 Wechseln der Datenquelle

Hier können Sie die IP-Adresse des Data Providers des Operation Centers wechseln. Die neuen Daten werden sofort übernommen.
Die Daten des Monitorings und die Backups der Konfigurationen werden dann in die Dienstdatenbank der neuen Adresse geschrieben.

- Klicken Sie im Bereich ***Operation Center*** auf die Schaltfläche ***Datenquelle***.
  Es öffnet sich das Fenster ***Datenquelle***, in dem die IP-Adresse des verwendeten Data Providers angezeigt wird.
- Tragen Sie in dem Feld ***IP*** die IP-Adresse des Rechners ein, dessen Data Provider Dienst Sie nutzen möchten.
- Ändern Sie im Feld ***Port*** die Portnummer falls nötig. Standardmäßig wird der Port 6178 benutzt.
- Klicken Sie auf ***Verbindung testen***. Erscheint nach ein paar Sekunden die Meldung ***OK*** neben der Schaltfläche, können die Daten mit der Schaltfläche ***Speichern*** gesichert werden.
- Wenn keine Verbindung hergestellt werden kann, überprüfen Sie die IP-Adresse und den Port. Stellen Sie sicher, dass der Dienst auf dem Zielrechner aktiviert und erreichbar ist.

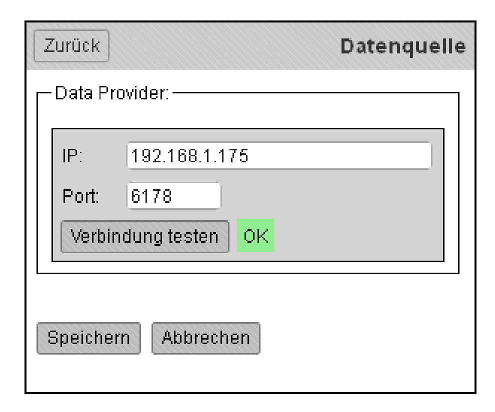


Abb. 81 Data Provider wechseln

8 Service Center

Im Menü ***Service Center*** werden die verfügbaren Dienste gelistet, die auf den eingestellten Data-Provider zugreifen. Auch Dienste anderer Rechner können auf den lokalen Datenprovider zugreifen. Daher ist jeder Dienst mit der IP-Adresse des ausführenden Rechners aufgeführt.

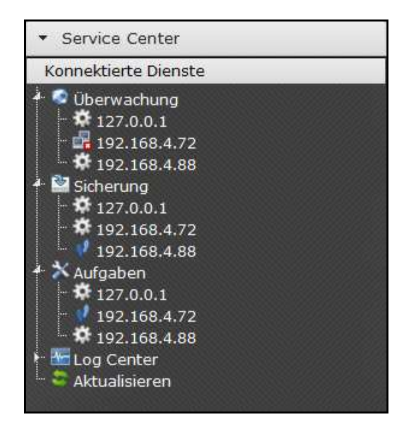


Abb. 82 zugreifende Dienste

In diesem Menü können Sie den Zugriff von anderen Rechnern reglementieren. Sie können für jeden Dienst festlegen, ob dieser den Datenprovider abfragen darf oder nicht. Außerdem können Sie festlegen, mit welcher Benutzerkennung sich der jeweilige Dienst mit dem Datenprovider verbinden darf.

Wenn Sie den Zugriff verweigern, wird der Dienst auf dem jeweiligen Rechner beendet. Wird der Dienst vom Benutzer neugestartet, wird dieser wieder beendet, solange er auf der Liste als ***Rejected*** (abgewiesen) geführt ist. Wird der Dienst aus der Liste entfernt, kann über die Zugriffserlaubnis neu entschieden werden.

Icon	Bedeutung
	Der Dienst wartet auf Erlaubnis, auf den Datenprovider zugreifen zu dürfen. Er ist weder abgelehnt noch erlaubt.
	Dem Dienst ist der Zugriff auf den Datenprovider gestattet.
	Der Dienst ist ***Rejected*** und auf dem entsprechenden Rechner gestoppt.

Um die Dienste auf einen anderen Datenprovider zu lenken, müssen Sie die Datei ***settings.dat*** bearbeiten. Die Datei finden Sie im ***Security Operation Center*** Ordner.

z. B.: `../Programme/Security Operation Center/bin/settings.dat`

- Öffnen Sie die Datei mit einem Editor und ändern Sie die Zeile:
  `data-ip=127.0.0.1`
- Setzen Sie die IP-Adresse des betreffenden Datenproviders ein.
  z. B.: `data-ip=192.168.175.10`

8.1 Dienst zulassen/abweisen

- Klicken Sie mit der ***rechten Maustaste*** auf die IP-Adresse des zu bearbeitenden Dienstes.
  Wählen Sie aus dem Kontextmenü den Eintrag ***Eigenschaften***.
  Es öffnet sich der Dialog ***Service Settings***.
- Klicken Sie Auf den Button ***Reject***, um den Dienst abzuweisen. Bestätigen Sie die Sicherheitsabfrage.
- Oder klicken Sie auf ***Allow***, um den Dienst den Zugriff zu erlauben. Es öffnet sich eine weitere ***Detailansicht***. Hier können Sie entscheiden, mit welcher ***Nutzerkennung*** sich der Dienst am Datenprovider anmeldet.
- Klicken Sie auf ***Speichern***, um zum Menü ***Service Center*** zurückzukehren.

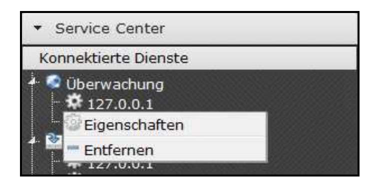


Abb. 83 Kontextmenü

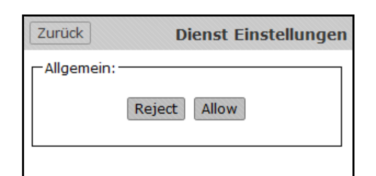


Abb. 84 Zugriff erlauben oder verweigern



Abb. 85 Benutzerkennung wählen

9 Link Center

Im Menü ***Link Center*** können Sie Internetadressen einzelner Webseiten speichern, um diese im SOC anzeigen zu lassen. Dies ist für externe Monitoring Dienste gedacht (z. B. MRTG), die über ein Webinterface aufgerufen werden. Die Funktion ist nicht als Browser-Ersatz gedacht, obwohl rudimentäre Browser-Funktionen verfügbar sind.
Außerdem können Sie Fernwartungsverbindungen speichern und diese im SOC anzeigen. Unterstützt werden das Protokoll RDP (remote desktop protocol) und die Software VNC (virtual network computing).
Wenn Sie einen HTTP-Proxy verwenden, müssen Sie die Einstellungen für den Proxy im Menü ***Operation Center*** im Untermenü ***Einstellungen*** vornehmen.
Hinweis: NTLM Authentifizierung wird nicht unterstützt.



Abb. 86 geöffneter externer Link

Die Adressen werden in einer Liste angezeigt, die alphabetisch nach den vergebenen Namen geordnet ist. Die Liste ist zur besseren Übersicht in Abschnitte der Anfangsbuchstaben gegliedert. Mit dem Eintrag ***Aktualisieren*** können Mitglieder einer Benutzergruppe prüfen, ob ein anderer Benutzer zwischenzeitlich neue Adressen für die Benutzergruppe hinzugefügt hat.

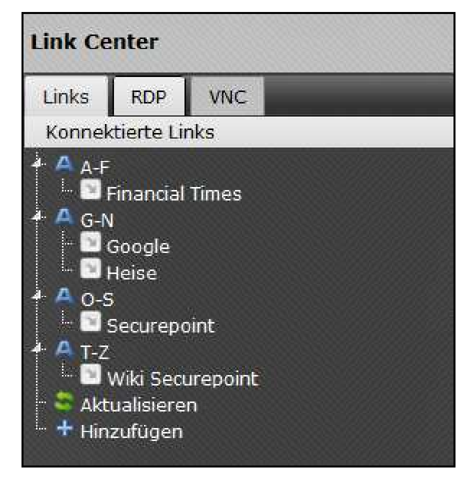


Abb. 87 Link Liste im Link Center

Die gleiche Struktur finden Sie unter den Registerkarten ***RDP*** und ***VNC*** für die Fernwartungsverbindungen.

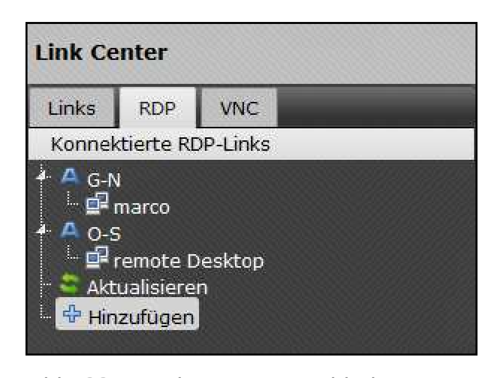


Abb. 88 angelegte RDP Verbindungen



Abb. 89 Liste angelegter VNC Verbindungen

9.1 Link hinzufügen

- Klicken Sie im Menü ***Link Center*** in der Registerkarte ***Link*** auf den Eintrag ***Hinzufügen***, um eine neue Internetadresse aufzunehmen.
  Es öffnet sich die Maske ***URL hinzufügen***.
- Geben Sie im Feld ***Name*** eine Bezeichnung für die neue Adresse ein.
- Im Feld ***URL*** geben Sie die vollständige Internetadresse an.
  Wenn Sie die Protokollangabe nicht mit angeben, wird die Adresse um den Eintrag ***http://*** ergänzt. Möchten Sie eine ***SSL***-Verbindung nutzen, müssen Sie das Protokoll (***https://***) angeben, da es sonst falsch interpretiert wird.
- Im Feld ***Benutzergruppen*** können Sie den Zugriff auf die Adresse auf eine bestehende Benutzergruppe des Operation Centers beschränken.
- Im Feld ***Useragent*** können Sie den zu verwendenden Browser einstellen.
  Standardmäßig wird der Browser Webkit benutzt. Manche Internet Seiten verlangen allerdings einen bestimmten Browser, den Sie dann hier auswählen können.
- Die Felder ***Benutzer*** und ***Kennwort*** müssen nur eingegeben werden, wenn die Internetseite mit einer Benutzerauthentifizierung gesichert ist.
- Klicken Sie abschließend auf ***Speichern***.

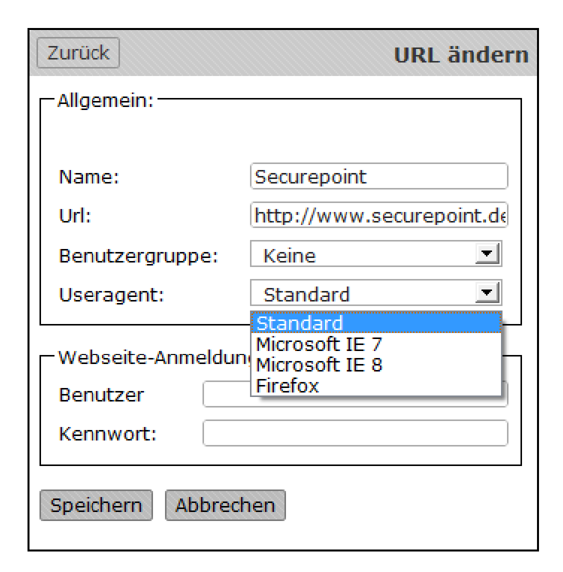


Abb. 90 externe Adresse hinzufügen

9.2 Fernwartungsverbindung hinzufügen

In den Registerkarten ***RDP*** und ***VNC*** werden die Verbindungen zur Fernwartung angezeigt.

- Klicken Sie im Menü ***Link Center*** in der Registerkarte ***RDP*** oder ***VNC*** auf den Eintrag ***Hinzufügen***, um eine neue Rechneradresse aufzunehmen.
  Es öffnet sich die Maske ***RDP Remote hinzufügen*** bzw. ***VNC Remote hinzufügen***.
- Geben Sie im Feld ***Name*** eine Bezeichnung für die neue Adresse ein.
- Im Feld ***URL*** geben Sie die vollständige Internetadresse an.
  Wenn Sie die Protokollangabe nicht mit angeben, wird die Adresse um den Eintrag ***http://*** ergänzt. Möchten Sie eine ***SSL***-Verbindung nutzen, müssen Sie das Protokoll (***https://***) angeben, da es sonst falsch interpretiert wird.
  Sie können natürlich auch eine ***IP-Adresse*** eingeben.
- Im Feld ***Benutzergruppen*** können Sie den Zugriff auf die Adresse auf eine bestehende Benutzergruppe des Operation Centers beschränken.
- Im Feld ***Widget-Größe*** können Sie die Größe des Fensters einstellen, in dem die Oberfläche des entfernten Systems angezeigt wird.
  Die Größe ist in Pixeln angegeben.
- Klicken Sie abschließend auf ***Speichern***.

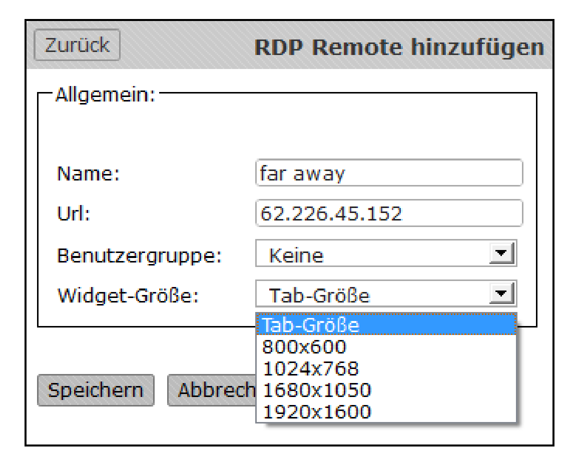


Abb. 91 Remote Desktop Protocol Verbindung

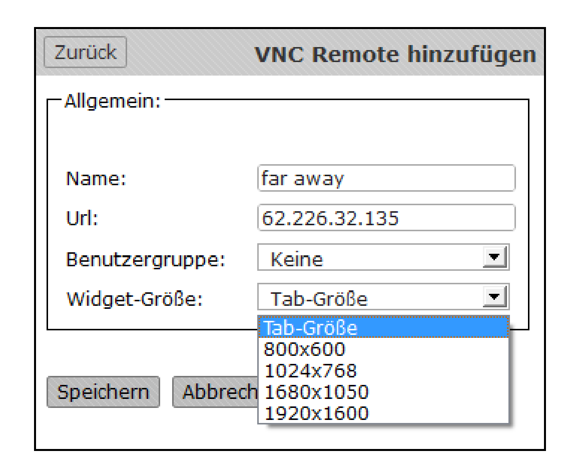


Abb. 92 Virtual Network Computing Verbindung

10 Log Center

Mit dem neuen Dienst ***Securepoint Logserver Service*** ist das Securepoint Log Center im Operation Center abrufbar.
Das Log Center zeichnet Syslog Protokolldaten der Firewalls auf, die die IP-Adresse des Log Center im Bereich ***Syslog*** der ***Servereigenschaften*** eingetragen haben.
Das Log Center zeichnet die Protokolldaten auf und archiviert diese in vorgegebenen Intervallen. Archivierte Daten werden für einen wählbaren Zeitraum vorgehalten und danach gelöscht.
Das Log Center versendet auf Wunsch tägliche Bericht-E-Mails, Alarm-E-Mails und Ereignis-E-Mails zu selbstdefinierten Ereignissen.

Im Menü ***Log Center*** finden Sie alle verfügbaren Log Center. Standardmäßig ist nur das lokale Log Center aufgeführt, da sich dieser mit dem lokalen Data Provider Dienst verbindet.

- Wenn Sie weitere Log Center von anderen Rechnern und Server mit dem lokalen Dienst verbinden möchten, müssen Sie die ***logserver.ini*** Datei der anderen Log Center bearbeiten.
- Wenn Sie den Installationspfad nicht geändert haben, finden Sie die Datei unter dem Pfad:
  `C:/Programme/Security Operation Center/bin/logserver.ini`
- Öffnen Sie die Datei in einem Editor und passen Sie Die Zeile ***useLocal*** und ***ip*** an.
- Setzen Sie für ***useLocal*** den Wert 0 und tragen Sie unter ***ip*** die IP-Adresse des Rechners ein, der das Log Center verwalten soll.
  ```
  [DataProvider]
  useLocal=0
  ip=192.168.175.175
  port=6178
  ```
- Nach einem Neustart des Operation Centers, wird das entfernte Log Center im Menü ***Log Center*** angezeigt.

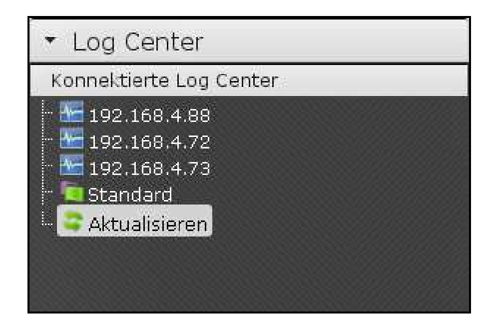


Abb. 93 Log Center Menü

10.1 Log Center Einstellungen

Die Einstellungen des Log Centers sind thematisch in drei Registerkarten aufgeteilt.

10.1.1 Registerkarte Allgemein

Bezeichnung	Beschreibung
Allgemeine Einstellungen	
Port	Portnummer, den das Log Center benutzt. voreingestellt: 9999
letzte Archivierung	Zeitpunkt der letzten Archivierung
Archivierungs-intervall	Zeitraum zwischen den Archivierungsläufen. Bei Eintrag ***Kein*** wird nicht archiviert.
Archivordner	Ordner, in dem die Archivierungsdaten abgelegt werden. Standardpfad: C:\Programme\SecurityOperationCenter\bin\lc Läuft das Log Center auf einem entfernten System, muss auch der Ordner auf dem System gespeichert werden.
letzte Säuberung	Letzter Zeitpunkt der Löschung veralteter Archivdaten.
Tageslimitierung	Zeitraum, die die Archivdaten vorgehalten werden. Beim Eintrag ***0*** Tage werden keine Daten vorgehalten.
Loggröße	Maximale Größe der Datenbank. Wird diese überschritten, werden die ältesten Einträge gelöscht bzw. archiviert.
DB Pfad	Geben Sie hier den kompletten Pfad der Datenbank mit Dateiname an. Standardpfad: C:\Programme\SecurityOperationCenter\bin\lc Läuft das Log Center auf einem entfernten System, muss auch die Datei auf dem System gespeichert werden.
Debug-Modus	Generiert eine Textdatei über die Aktivitäten des Log Center.
Letzter Dienst	
Logeinträge	Maximale Anzahl der Logeinträge. Wird die gewählte Zahl überschritten, werden die ältesten Einträge gelöscht bzw. archiviert.
Syslog Einstellungen	
IP	IP-Adresse des Syslog Servers
Port	Port des Syslog Servers

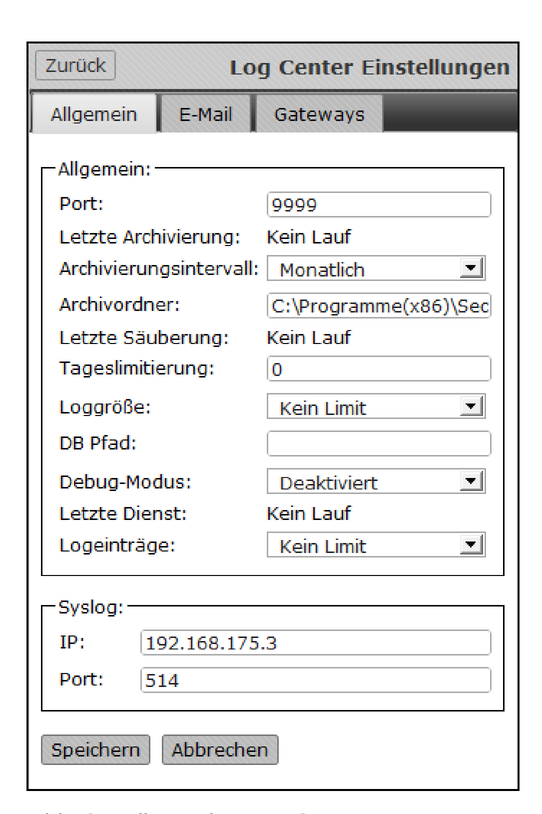


Abb. 94 allgemeine Log Center Einstellungen

10.1.2 Registerkarte E-Mail

Auf der Registerkarte ***E-Mail*** wird eingestellt, von welchem Mails Server und mit welcher Absenderadresse E-Mails für Ereignisse, Alarmbenachrichtigungen und Berichte gesendet werden.
Zusätzlich können noch Benutzerdaten für die SMTP Authentifizierung hinterlegt werden, wenn der Server dies erfordert.

Bezeichnung	Beschreibung
Ereignisemail	
Von	E-Mail-Adresse des Absenders
Server	IP-Adresse oder Hostname des Mail Servers
Alarmemail	
Von	E-Mail-Adresse des Absenders
Server	IP-Adresse oder Hostname des Mail Servers
Berichtsemail	
von	E-Mail-Adresse des Absenders
Server	IP-Adresse oder Hostname des Mail Servers
Uhrzeit	Zeitpunkt, zu dem die Berichts-E-Mail erstellt und versandt werden soll.
SMTP Authentifizierung	
Aktivieren	Checkbox zur Aktivierung der Authentifi-zierung
Login	Benutzername am Mail Server
Kennwort	Kennwort zur Anmeldung am Mail Server



Abb. 95 E-Mail Einstellungen des Log Centers

10.1.3 Registerkarte Gateways

Auf der Registerkarte ***Gateways*** werden die Appliances gelistet, die ihre Protokolldaten an den Logserver senden.
Wenn Sie auf den Button ***Hinzufügen*** klicken, wird eine Liste aller eingetragener Appliances angezeigt. Hier können Sie auswählen, welche Maschinen Protokolldaten an den Log Server senden sollen.

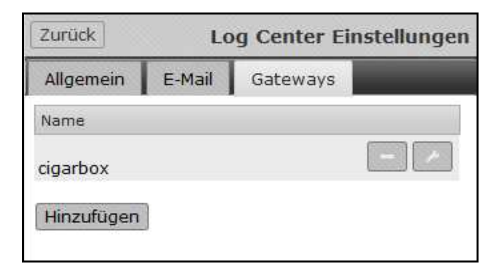


Abb. 96 Liste der zugewiesenen Appliances

Wenn Sie auf das ***Werkzeugschlüsselsymbol*** einer ausgewählten Appliance klicken, öffnet sich der Bereich ***Berichtseinstellungen*** mit den Registerkarten ***Generierung*** und ***E-Mail***.
Auf der Registerkarte ***Generierung*** können Sie auswählen, zu welchen Protokolldaten der Appliance Berichte generiert werden sollen und in welchen Intervallen dieses geschehen soll.
Als Intervalle stehen täglich, wöchentlich, monatlich und jährlich zur Auswahl. Diese Intervalle sind auch kombinierbar.

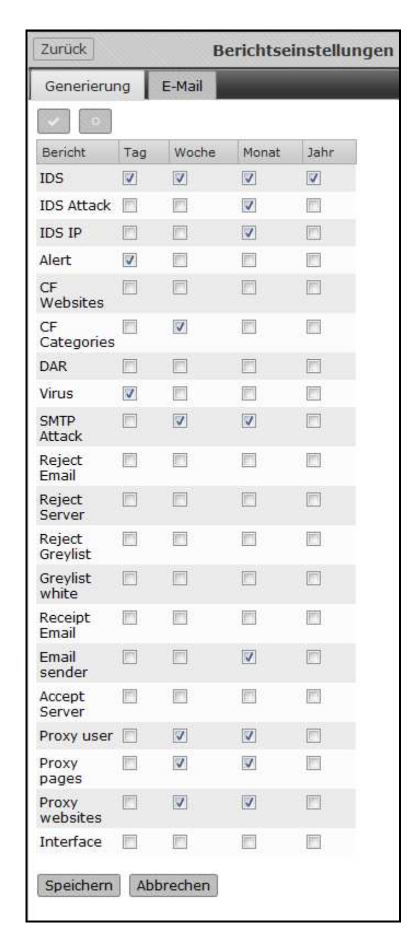


Abb. 97 Erstellung der Berichte

Auf der Registerkarte E-Mail können Sie entscheiden, wann die erstellten Berichte versendet werden. Dies steht in Abhängigkeit zu den Generierungseinstellungen: Es können nur täglich Berichte gesendet werden, wenn diese auch täglich erstellt werden.

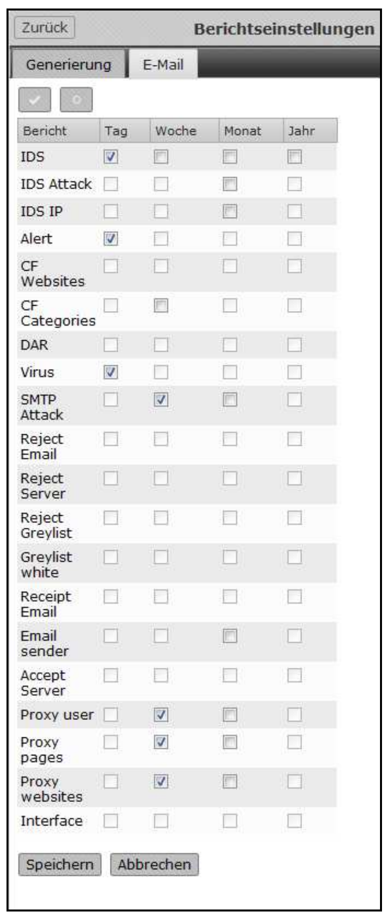


Abb. 98 Versandintervalle der Berichte

Die auf der vorherigen Seiten beschriebenen Einstellungen erreichen Sie über das Kontextmenü des jeweiligen Log Centers im Menü ***Log Center***.

Außerdem befindet sich im Menü noch der Eintrag ***Standard***. Unter diesem Eintrag gespeicherte Daten werden für jedes neue Log Center gesetzt. Die Einstellungen erreichen Sie ebenfalls über das Kontextmenü.

10.2 Kontextmenü eines Log Centers

Über das Kontextmenü des Log Centers erreichen Sie weitere Einstellungen für das jeweilige Log Center.

Bezeichnung	Beschreibung
Verbinden	Öffnet den Log-Client und verbindet sich mit dem Log Center.
Eigenschaften	Einstellungen des Log Centers bearbeiten.
E-Mail-Empfänger	E-Mail-Empfänger festlegen für die E-Mail-Benachrichtigungen des Log Centers.
Ereignis-Einstellung	Öffnet einen Dialog zum Definieren von Ereignissen.
Löschen	Den Log Center aus der Liste löschen.

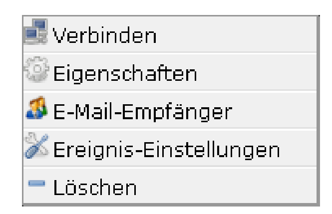


Abb. 99 Kontextmenü eines Log Centers

10.3 E-Mail-Empfänger einstellen

Für die verschiedenen Benachrichtigungen per E-Mail können Sie Empfänger festlegen. Bedingung für das Hinzufügen von Empfängern ist, dass diese als Benutzer im Security Operation Center eingetragen sind und eine E-Mail-Adresse in der Benutzerverwaltung hinterlegt ist.

- Klicken Sie im Menü ***Log Center*** mit der rechten Maustaste auf das Log Center, für den Sie E-Mail-Empfänger hinzufügen möchten.
- Klicken Sie im Kontextmenü auf den Eintrag ***E-Mail-Empfänger***.
  Es öffnet sich der Dialog ***E-Mail-Empfänger*** mit den Registerkarten ***Alarm***, ***Ereignis*** und ***Bericht***.
- Wählen Sie die entsprechende Registerkarte für die gewünschte Benachrichtigung und klicken Sie auf den Button ***Hinzufügen***.
  Es öffnet sich der Dialog ***Empfänger hinzufügen***.
- Um einen Benutzer zur Empfängerliste hinzuzufügen, klicken Sie auf den Button mit dem ***Plussymbol*** des jeweiligen Benutzers.
- Haben Sie alle gewünschten Empfänger eingetragen, gelangen Sie mit dem Button ***Zurück*** zum vorherigen Dialog.
- Wiederholen Sie diese Aktion ggf. für die weiteren Benachrichtigungen.

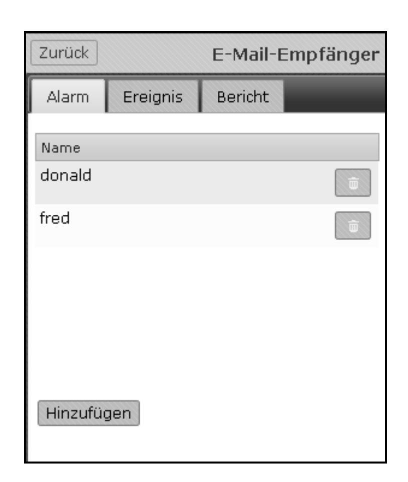


Abb. 100 eingetragene Empfänger



Abb. 101 Empfängerauswahl

10.4 Ereignisse definieren

Sie können selber Ereignisse definieren, bei deren Auftreten das Log Center eine E-Mail sendet.

- Klicken Sie im Menü ***Log Center*** mit der rechten Maustaste auf das Log Center, für den Sie Ereignisse definieren möchten.
- Klicken Sie im Kontextmenü auf den Eintrag ***Ereignis-Einstellungen***.
  Es öffnet sich der Dialog ***Log Center Ereignisse*** mit einer Liste der erstellten Ereignisse.
- Um ein neues Ereignis zu definieren, klicken Sie auf den Button ***Hinzufügen***.
  Es öffnet sich der Dialog ***Log Center Ereignis***.
- Geben Sie im Feld ***Namen*** eine Bezeichnung für das Ereignis an.
- Wählen Sie aus der ***Dropdownbox*** einen Dienst auf den dieses Ereignis zutreffen soll.
- Geben Sie im Feld ***Regex*** einen Regulären Ausdruck an, nach dem die Nachrichtenzeilen durchsucht werden.
- Aktiviren Sie das Ereignis mit der Checkbox ***Active***.
- Geben Sie im Feld ***Nachricht*** einen Text ein, der in der E-Mail-Nachricht mit einfließen soll.
- Die Erstellung ist abgeschlossen, wenn Sie auf ***Speichern*** klicken.

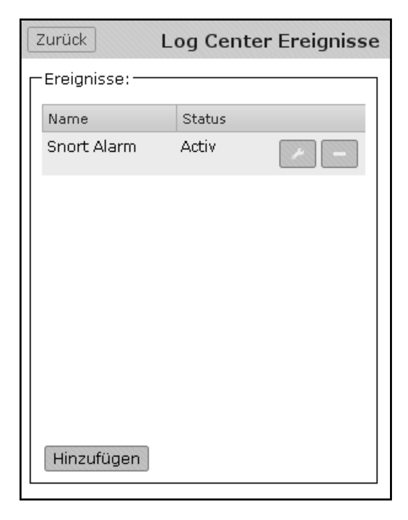


Abb. 102 eingestellte Ereignisse



Abb. 103 Ereignis erstellen

11 Gateway Center

In diesem Bereich werden alle eingetragenen Gateways aufgelistet. Dies umfasst nicht nur UTM und VPN Gateways. Auch Geräte wie UMA (Unified Mail Archive), NAC (Network Access Controller) und Miriam (Multi Interface Router mit integrierter Aufdeckung von Manipulation) werden auf unterschiedlichen Registerkarten geführt.
Die Gateways können nach verschiedenen Kriterien geordnet werden z. B. Name, Typ, Gruppenzugehörigkeit usw.

Mit einem Doppelklick auf ein Gateway initiieren Sie eine Verbindung zu dem Gerät. Das Verwaltungsinterface des Gerätes wird im rechten Fenster gestartet.
Sind Sie mit einem oder mehreren Gateways verbunden, werden diese grün hinterlegt.



Abb. 104 Gateways nach Gruppen geordnet

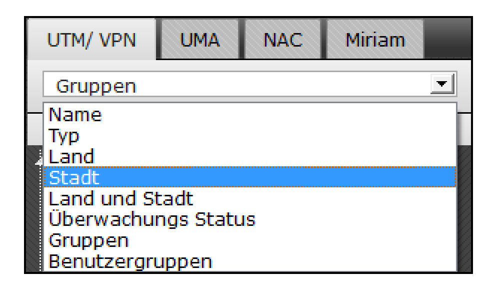


Abb. 105 Gruppierungsoptionen

11.1 CLI Log

Ist das Operation Center mit einem UTM- oder VPN-Gateway verbunden, wird die Ein- und Ausgaben der Kommunikation zwischen Operation Center und Firewall im CLI-Log (Command Line Interface) protokolliert. Im rechten Fenster kann diese Protokollierung über die Registerkarte ***CLI-Log*** angezeigt werden.

Die Protokollierung dient der Kontrolle und Analyse der Kommunikation.

Es entspricht der Funktion, die auch das Administrations-Webinterface unter dem Menüpunkt ***Extras*** anbietet. Diese Protokollierung ist nicht auf 100 Einträge beschränkt, sondern auf 10 MB.

Über das Kontextmenü können Sie die Einträge in die Zwischenablage kopieren, markieren oder das automatische Scrollen zum aktuellen Eintrag aktivieren und deaktivieren.



Abb. 106 aktivierte Registerkarte CLI-Log

11.2 SSH-Konsole

Bei der Verbindung mit einem UTM- oder VPN-Gateway wird die Registerkarte ***SSH Konsole*** angezeigt.
Auf dieser Registerkarte können sie direkt CLI Kommandos an das Gateway senden. Tragen Sie die Befehle in die Befehlsleiste unter dem rechten Fenster ein und klicken Sie zum Übertragen auf den Button ***Senden***.
Dies entspricht der Funktion, die auch das Administrations-Webinterface unter dem Menüpunkt ***Extras*** anbietet.

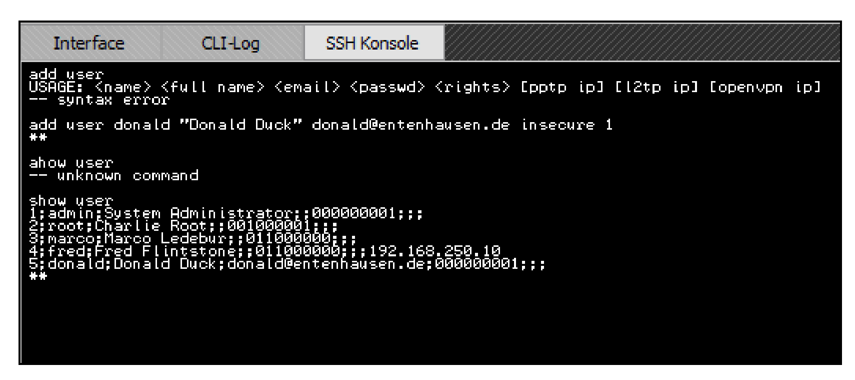


Abb. 107 Senden von CLI Befehlenüber die SSH Konsole

11.3 Kontextmenü

Zu jedem Gateway können Sie ein Kontextmenü aufrufen, welches Optionen zur Bearbeitung des Gateways beinhaltet.

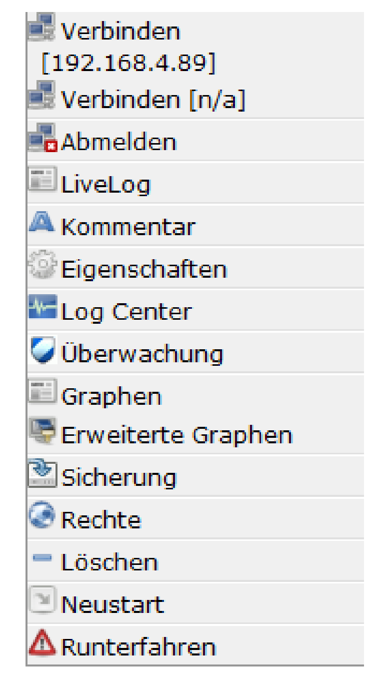


Abb. 108 Kontextmenü eines Gateway

Bezeichnung	**Funktion**
Verbinden	Verbindung zum Gateway mit den gespeicherten Zugangsdaten aufbauen.
Abmelden	Verbindung zum Gateway trennen.
LiveLog	Öffnet ein neues Fenster, in dem das Live Log des jeweiligen Gateway ausgeführt wird.
Kommentar	Beschreibung oder Anmerkung zum Gateway.
Eigenschaften	Öffnet einen Dialog zur Bearbeitung der Eigenschaften des Gateway.
Log Center	Server, die Protokolldaten dieser Appliance loggen, anzeigen und hinzufügen.
Überwachung	Zeigt eine Liste der gespeicherten Überwachungsläufe.
Graphen	Öffnet Graphen für die CPU-Last, Speicher- und SWAP-Nutzung.
Erw. Graphen	Öffnet Graphen für TCP- und UDP-Verbindungen und den Online Status.
Sicherung	Zeigt angelegte Sicherungen an.
Rechte	Zeigt Zugriffsrechte von Gruppen und Benutzer auf die Firewall.
Löschen	Gateway aus der Liste löschen.
Neustart	Gateway neu starten.
Runterfahren	Gateway abschalten.

11.4 Suchmaske

Am unteren Rand finden Sie eine Suchmaske. Sie können Gateways nach Namen oder IP-Adressen suchen. Ist die Suche erfolgreich, wird das gefundene Gateway farbig markiert. Außerdem sind hier Schaltflächen platziert, mit denen Sie alle Gruppierungen öffnen oder schließen können.

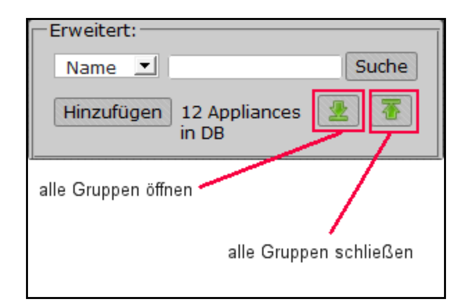


Abb. 109 Suchmaske im Bereich UTM/VPN Gateway

11.5 Gateway hinzufügen

In der gleichen Maske finden Sie den Button ***Hinzufügen***, mit dem Sie ein neues Gateway anlegen können.

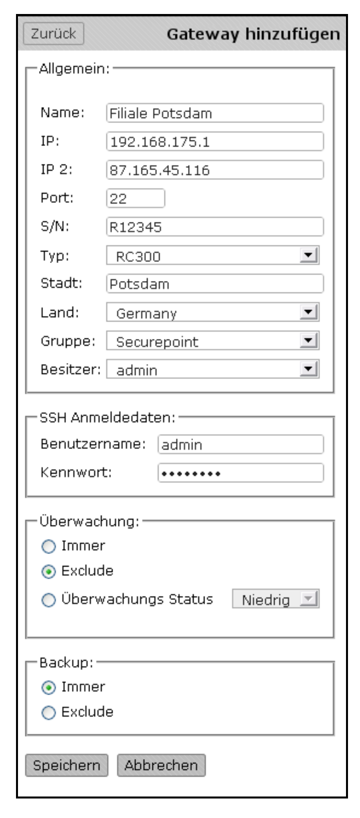


Abb. 110 Gateway hinzufügen

Bezeichnung	Beschreibung	
Name	Name der neuen Appliance	
IP und IP2	IP-Adressen der Appliance (zum Beispiel interne und externe IP-Adresse)	
Port	Zu benutzender SSH Port (Standard 22)	
S/N	Seriennummer der Appliance	
Typ	Wahl des Appliance Typs	
Stadt	Standort der Appliance	
Land	Standort der Appliance	
Gruppe	Wählen Sie die Gruppenzugehörigkeit.	
Besitzer	Wählen Sie den Besitzer der Appliance.	
SSH	Benutzername	Benutzername für die SSH-Verbindung
	Kennwort	Kennwort für die SSH-Verbindung
Überwachung	Immer	Appliance wird ständig überwacht.
	Exclude	Appliance wird von der Überwachung ausgeschlossen.
	Status	Setzen Sie den Überwachungsstatus (niedrig, normal, wichtig).
Backup	Immer	Konfigurationssicherungen werden immer angelegt.
	Exclude	Die Appliance wird von der Sicherung ausgenommen.

11.6 Kontextmenü Eintrag Log Center

Hier können Sie IP-Adressen von Servern angeben, auf denen der Dienst ***Securepoint Logserver Service*** läuft. Sind hier IP-Adressen eingetragen, werden von dem Dienst alle Protokolleinträge angenommen und in eine Datenbank geschrieben.
Mit dem integrierten Logclient können Sie die aufgezeichneten Logeinträge einsehen und ein Echtzeitlog betrachten.

- Zum Eintragen eines Log Centers klicken Sie im Kontextmenü einer Firewall auf den Eintrag ***Log Center***.
- Es wird das Fenster ***Gateway Log Center*** eingeblendet.
- Hier werden alle eingetragenen Log Center ange*zeigt. Wenn für das Gateway noch kein Log Center* eingetragen ist, ist die Liste leer.
- Um einen Log Center einzutragen, klicken Sie auf ***Hinzufügen***. Es öffnet sich der Dialog ***Log Center hinzufügen***.
- Wählen Sie auf der Liste der ***verfügbaren Log Center*** einen Log Center aus und klicken Sie auf das Icon mit dem ***Plussymbol***. Wiederholen Sie dies, wenn Sie mehrere Log Center eintragen möchten.
- Klicken Sie auf ***zurück***.
- Sie können jetzt die IP-Adressen der gewählten Log Center an das Gateway senden. Dann werden die IP-Adressen auf das Gateway im Bereich Servereinstellungen gespeichert.
  Dies machen Sie mit dem Button ***Übertragen***. Es werden nur neue Einträge übertragen, keine bestehenden auf den Gateway überschrieben.
- Klicken Sie auf ***zurück***.



Abb. 111 Liste der eingetragenen Log Center

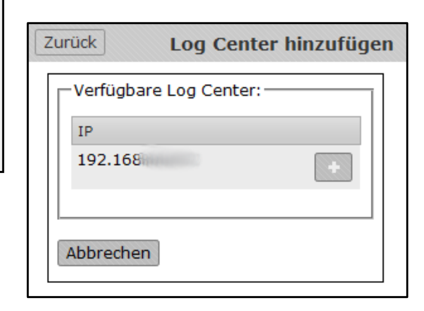


Abb. 112 Log Center auswählen

11.7 Kontextmenü Eintrag Graphen

Über die Einträge ***Graphen*** und ***erweiterte Graphen*** im Kontextmenü können Sie sich Last- und Verbindungsstatistiken grafisch anzeigen lassen. Es werden immer die letzten hundert Werte der Überwachung verwendet, soweit diese vorhanden sind.

Der Punkt ***Graph*** zeigt die Prozessorlast, die Arbeitsspeicherauslastung und die Auslagerungsdateiauslastung.

Der Punkt ***Erweiterte Graphen*** zeigt die Anzahl der TCP- und UDP-Verbindungen und den Online Status der Appliance.

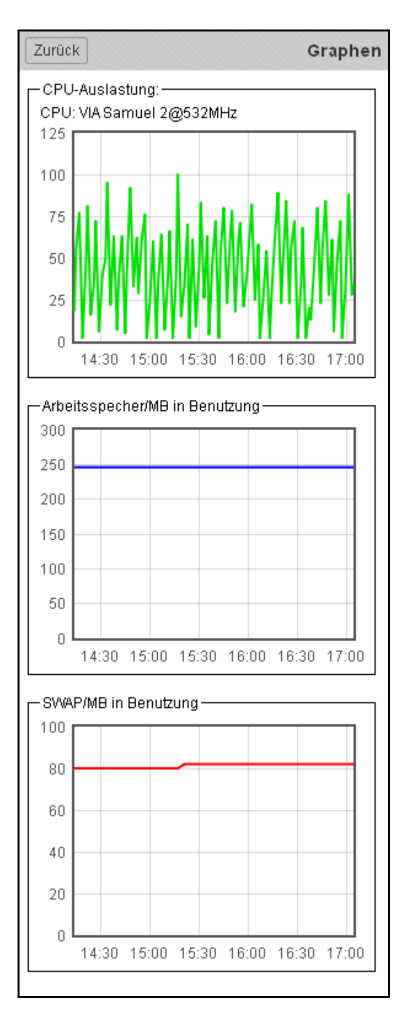


Abb. 113 Lastgraphen

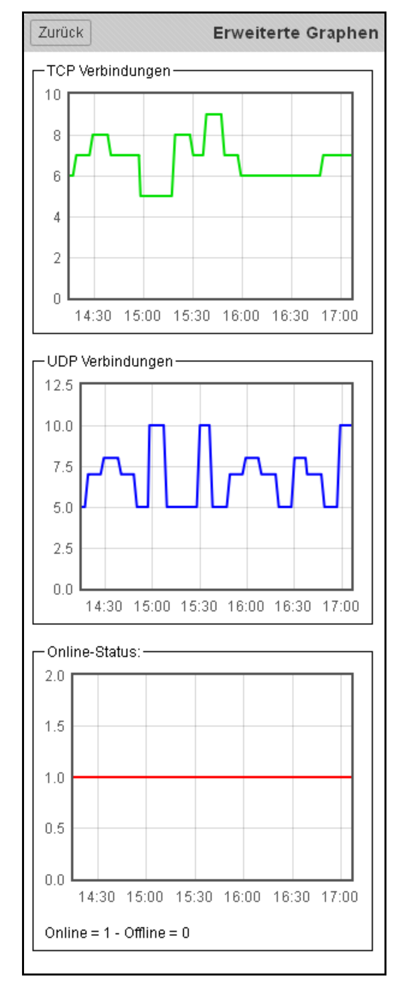


Abb. 114 Verbindungsgraphen

11.8 Kontextmenü Eintrag Sicherung

In diesem Bereich sind die angelegten Sicherungen aufgelistet (beginnend mit der neusten). Es werden pro Appliance immer nur zehn Sicherungen in der Datenbank gespeichert.

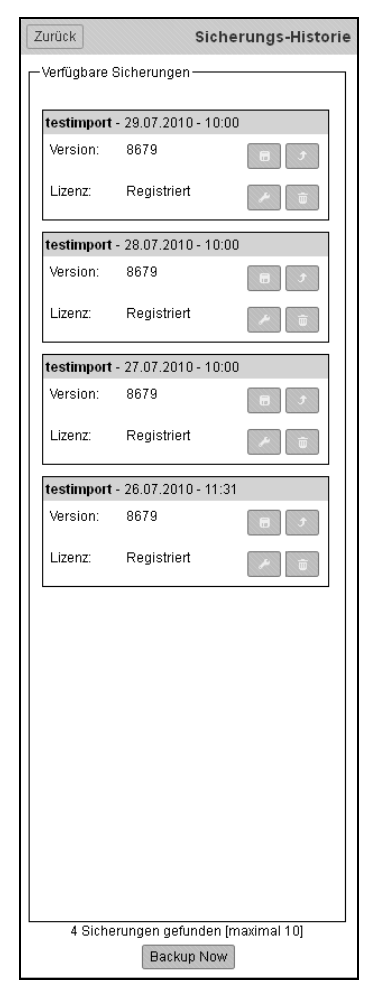


Abb. 115 Auflistung der Sicherungen

Neben dem Namen der gespeicherten Konfiguration wird das Datum und die Uhrzeit der Sicherung angezeigt.
Sie haben die Möglichkeit, Daten mit dem ***Export*** Button zu exportieren oder die Konfiguration auf die Appliance mit dem ***Upload*** Button zurückzuspielen. Dabei können Sie die Konfiguration unter einem neuen Namen zurückspielen oder den alten Namen übernehmen. Anschließend werden Sie gefragt, ob die Konfiguration als Startkonfiguration verwendet und die Appliance neu gestartet werden soll.

Mit dem ***Werkzeugschlüssel*** Symbol können Sicherungen bearbeitet werden. Die gespeicherte Sicherung wird im Webinterface geöffnet, und Sie können Einstellungen offline vornehmen. Sie bearbeiten also nicht die aktuell laufende Konfiguration.
Da es sich um Backups handelt, die im Offline Betrieb bearbeitet werden, sind einige Funktionen, wie z.B. die Konfigurationsverwaltung und das Live Log nicht verfügbar.
Die so veränderten gesicherten Konfigurationen können dann auf die Appliance zurückgespielt werden.

11.9 Kontextmenü Eintrag Rechte

Unter den Eintrag ***Rechte*** im Kontextmenü können Sie Zugriffsrechte für die Appliance setzen.
Die verfügbaren Rechte sind:

- Verweigern — Der Gruppe oder dem Benutzer wird die Ansicht auf diese Appliance verweigert.
- Lesen — Der Gruppe oder dem Benutzer steht die Appliance nur lesend zur Verfügung.
- Lesen / Schreiben — Die Gruppe oder der Benutzer darf die Einstellungen der Appliance lesen und bearbeiten.

Hinweis: Die Zugriffsrechte des Benutzers Überschreiben die Rechte der Gruppe.
Beispiel: Der Gruppe Mitarbeiter ist nur Leserecht gewährt. Der Benutzer A ist Mitglied der Gruppe Mitarbeiter. Ihm sind als Benutzer in der Benutzerverwaltung Lese- und Schreibrechte zugewilligt. Somit kann er lesend und schreibend auf die Appliances zugreifen, obwohl die Gruppe nur lesend zugreifen kann.



Abb. 116 Gruppen- und Benutzerrechte

12 Sidebar Menü

Als alternative Menüansicht wird das Sidebar Menü angeboten. Bei kleineren Bildschirmen oder kleinerer Auflösung hat dies den Vorteil, dass die meisten Dialoge ohne Scrollbalken auskommen, da die untereinander angeordneten Menüs entfallen.

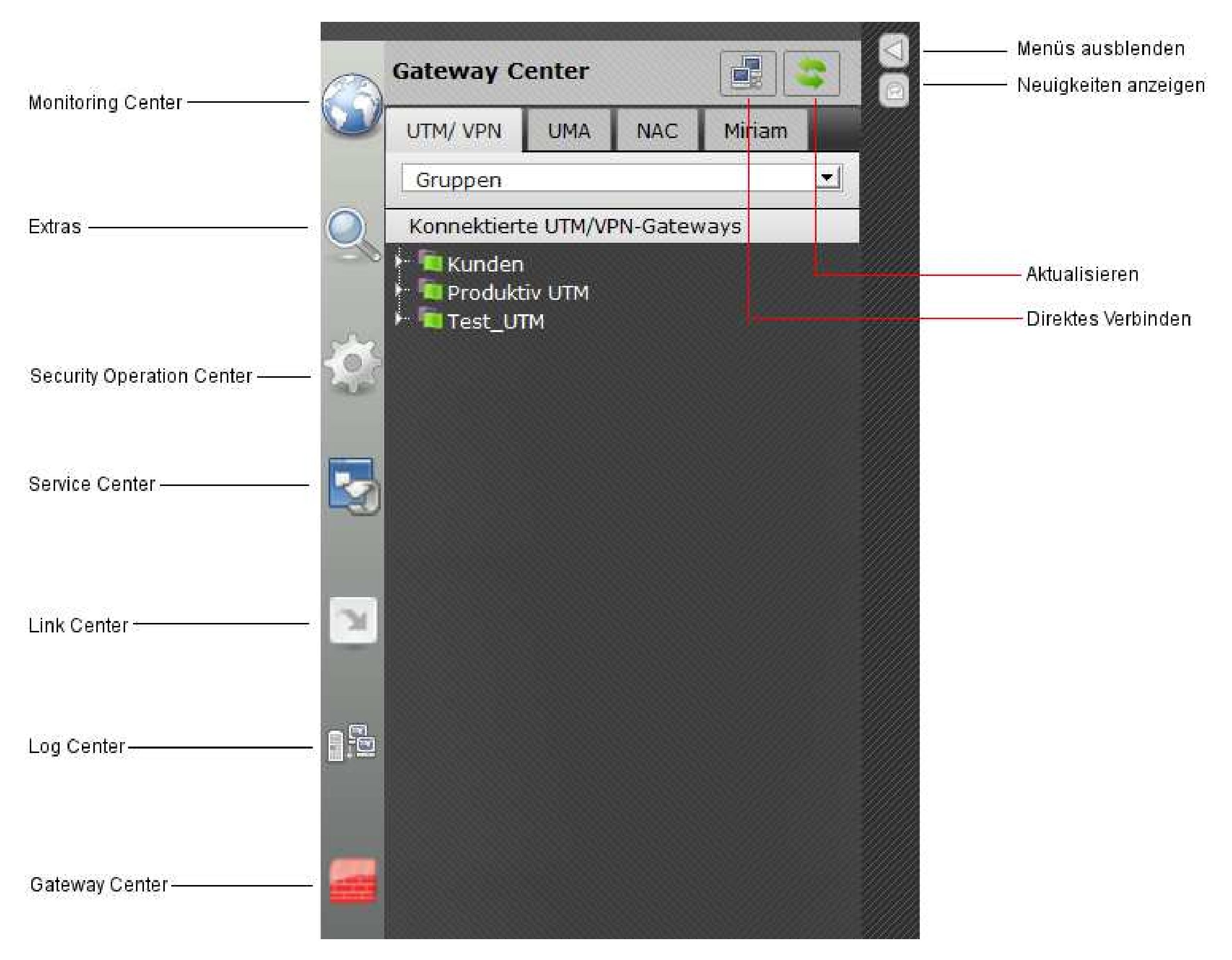


Abb. 117 Sidebar Menü

Im Menü ***Gateway Center*** finden Sie in dieser Ansicht die zusätzlichen Buttons ***Quick Connect*** und ***Refresh***, die in der anderen Ansicht nicht verfügbar sind.
Mit dem Button ***Refresh*** aktualisieren Sie die Ansicht der Gateway Liste.

12.1 Quick Connect

Mit der Funktion ***Quick Connect*** können Sie eine Verbindung zu einer Appliance aufbauen, die nicht dauerhaft in die Gateway-Liste aufgenommen werden soll.
Der Button ***Quick Connect*** öffnet einen Dialog, in dem Sie die Verbindungsdaten zum Gateway eingeben können.

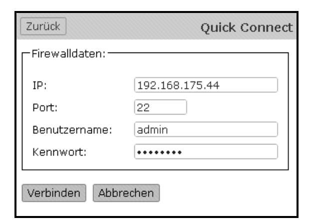


Abb. 118 Qick Connect Dialog

13 Securepoint Log Center Client

Ab der Version 2.0 des SOCs ist ein Logclient integriert, der nicht nur das Live Log zeigt, sondern auch historische Protokolldaten anzeigt.
Durch die Integration eines Log Centers im SOC können Protokolldaten von verschiedenen Appliances aufgenommen und im Logclient dargestellt werden. Der Logclient bietet verschiedene Filtermöglichkeiten für das Live Log und für das historische Log. Außerdem werden grafische und tabellarische Auswertungen der Logdaten angeboten.

- Sie erreichen den Logclient über das ***Kontextmenü*** eines Log Centers mit dem Eintrag ***Verbinden*** oder durch ein ***Doppelklick*** auf das Log Center.
- Es öffnet sich das Fenster ***Securepoint Log Center Client***.
- Es öffnet sich eine Verbindungsabfrage, in der Sie ggf. Benutzername und Kennwort für das Log Center eintragen müssen. In der Regel werden die Anmeldedaten vom SOC übergeben. Anmeldeberechtigt sind nur ***Benutzer mit Administratorrechten*** des SOCs.

Kommt eine Verbindung nicht zustande, überprüfen Sie die Anmeldedaten.
Versichern Sie sich, dass Sie den richtigen ***Data Provider*** Dienst benutzen.
Prüfen Sie, ob der Dienst ***Securepoint Logserver Service*** gestartet ist und ob dieser mit der Datei ***logserver.ini*** mit dem richtigen Data Provider verbunden ist (siehe Kapitel 10).

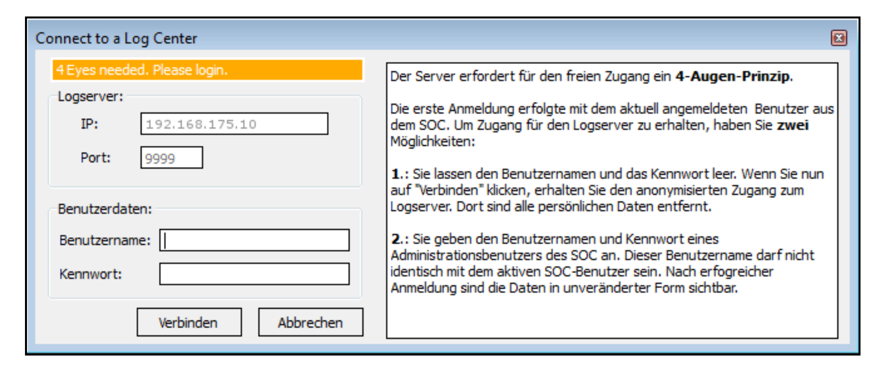


Abb. 119 Log Center-Verbindungsdaten

Hinweis: Die Verbindungsdaten müssen auf die jeweilig verwendete Log Center Version angepasst sein. Lesen Sie dazu das Kapitel 1.1 Log Center Versionen.

Im Fenster des Logclient können Sie am linken Rand zwischen den vertikalen Registerkarten ***Logging*** und ***Berichte*** wechseln. Auf dem Logging Tab werden Protokolleinträge aufgelistet. Der Berichte Tab bietet verschiedene Auswertung in grafischer und tabellarischer Form an.

In der Statusleiste am unteren Rand wird immer eingeblendet mit welchem Log Center Sie gerade verbunden sind, ob Filter gesetzt sind und wie viele Datensätze ausgewählt sind.

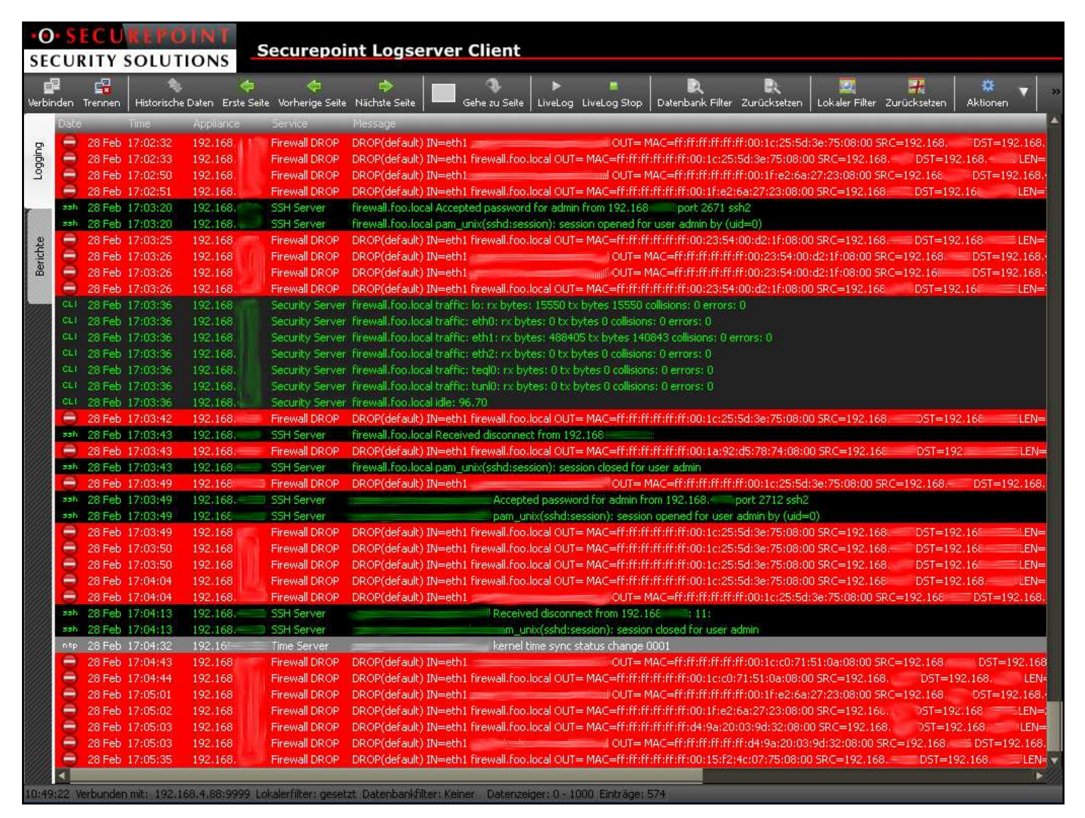


Abb. 120 Logclient Fenster

13.1 Logclient Icon-Leiste



Abb. 121 Iconleiste - linke Hälfte

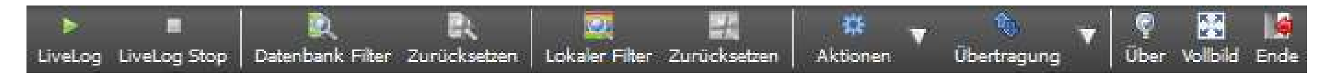


Abb. 122 Iconleiste - rechte Hälfte

<table>
<tr><th>Bezeichnung</th><th colspan="2">Beschreibung</th></tr>
<tr><td>Verbinden</td><td colspan="2">Verbindung mit einem Log Center aufbauen. Anmeldedialog zur Eingabe von IP-Adresse, Port und Anmeldedaten erscheint.</td></tr>
<tr><td>Trennen</td><td colspan="2">Trennt die aktuelle Verbindung.</td></tr>
<tr><td>Historische Daten</td><td colspan="2">Aufgenommene Protokolldaten aus der Datenbank laden.</td></tr>
<tr><td>erste Seite</td><td colspan="2">Springt zu ersten Seite der geladenen Daten.</td></tr>
<tr><td>vorherige Seite</td><td colspan="2">Lädt die vorherige Seite in Bezug zur aktuellen Seite der geladenen Daten.</td></tr>
<tr><td>nächste Seite</td><td colspan="2">Lädt die nächste Seite in Bezug zur aktuellen Seite der geladenen Daten.</td></tr>
<tr><td>Gehe zu Seite</td><td colspan="2">Geben Sie eine Seitennummer in Kästen links neben dem Icon ein und klicken Sie dann auf das Icon. Die Ansicht springt zur angegebenen Seite</td></tr>
<tr><td>Live Log</td><td colspan="2">Der Logclient zeigt fortlaufend die aktuellen Protokolldaten an.</td></tr>
<tr><td>Live Log Stop</td><td colspan="2">Anzeige der aktuellen Protokolldaten beenden.</td></tr>
<tr><td>Datenbank Filter</td><td colspan="2">Setzt einen Filter für Protokolldaten, die aus der Datenbank geladen werden. Der Filter gilt für das nächste Laden oder wenn Daten neu geladen werden.
Filteroptionen: Zeitraum, Appliance, Dienst, Nachricht, Inverser Filter</td></tr>
<tr><td>Zurücksetzen</td><td colspan="2">Setzt den Filter für die Datenbank zurück.</td></tr>
<tr><td>Lokaler Filter</td><td colspan="2">Setzt einen Filter für geladene Protokolldaten.
Filteroptionen: Datum, Zeitspanne, Appliance, Dienst, Nachricht, Inverser Filter</td></tr>
<tr><td>Zurücksetzen</td><td colspan="2">Setzt den Filter für geladene Daten zurück. Es werden wieder alle geladenen Daten angezeigt.</td></tr>
<tr><td rowspan="4">Aktionen</td><td>nach unten blättern</td><td>Die Ansicht zeigt beim Live Log immer die aktuellsten Einträge.</td></tr>
<tr><td>Daten beim Zurücksetzen holen</td><td>Daten werden beim Zurücksetzen des Filters neu geladen.
Gilt für den Datenbankfilter.</td></tr>
<tr><td>Ansicht löschen</td><td>Löscht die Daten aus dem Anzeigefenster.</td></tr>
<tr><td>Historische Log Zeilen</td><td>Beschränkt die Anzahl der geladenen Datensätze.
in tausender Schritten bis 5000, 10000 und 15000</td></tr>
<tr><td rowspan="3">Übertragung</td><td>Datenkomprimierung aktivieren</td><td>Daten werden vor der Übertragung zum Log Client komprimiert und vor der Anzeige im Log Client wieder dekomprimiert. Die Daten werden als ZIP Datei übertragen.</td></tr>
<tr><td>schnell</td><td>einfache Komprimierung</td></tr>
<tr><td>normal</td><td>normale Komprimierung</td></tr>
</table>

	maximal	hohe Komprimierung
Über	Zeigt Versionsnummer und Kontaktdaten.	
Vollbild	Wechselt die Ansicht zum Vollbild und zurück zur Fensteranzeige.	
Ende	Beendet den Logclient.	

13.2 Datenbank-Filter und Live-Log-Filter

Um die Protokolldaten gezielt zu analysieren, sind die implementierten Filter hilfreiche Werkzeuge. Es wird zwischen Datenbank-Filter und Live-Log-Filter (Lokaler Filter) unterschieden. Durch Setzen eines Wertes im Datenbank-Filter werden Daten schon beim Laden aus der Datenbank nach den definierten Gesichtspunkten selektiert.
Mit dem Lokalen Filter können die geladenen Log-Einträge weiter gefiltert werden.

Durch den Button ***Setzen und holen*** im Datenbank-Filter werden die Daten aus der Datenbank nach den eingestellten Kriterien sofort neu geladen. Wenn Sie dagegen den Button ***Setzen*** benutzen, werden die Daten erst aktualisiert, wenn Sie mit den Befehlen ***nächste Seite***, ***vorherige Seite*** und ***erste Seite*** durch die Daten navigieren oder durch den Button ***Historische Daten*** die Log Einträge neu laden.

Beim Lokalen Filter werden durch den Befehl ***Setzen*** die Daten sofort eingegrenzt.
Durch die Checkbox ***Case Sensitive*** werden die Nachrichteneinträge unter der Beachtung der Groß- und Kleinschreibung gefiltert.

Durch die Checkbox ***Invertieren*** werden nur Daten gezeigt, auf denen die gesetzten Kriterien **nicht** zutreffen.

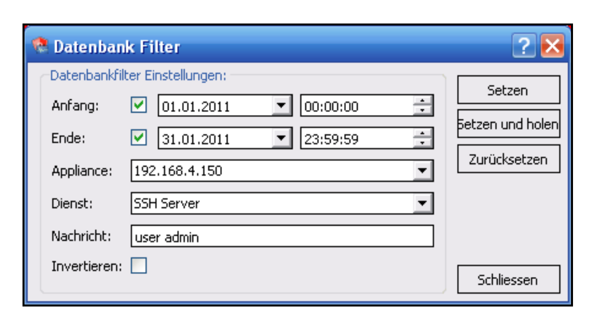


Abb. 123 Datenbank Filter

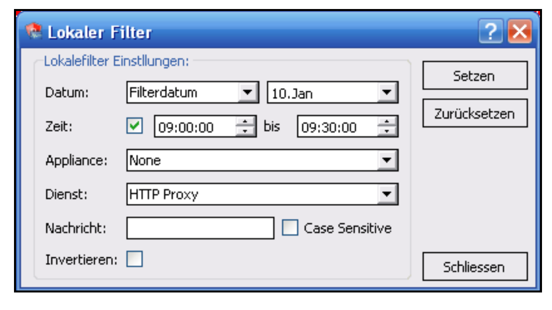


Abb. 124 Lokaler Filter

13.3 Berichte des Log Clients

Der Logclient erstellt aus den Protokolldaten Berichte für jede eingetragene Appliance. Die Berichte werden tabellarisch, grafisch oder gemischt dargestellt. Es werden Daten für die letzten 24 Stunden, die letzte Woche und den letzten Monat angezeigt.
Unter dem Bereich ***Berichtsarchiv*** können Sie auch ältere Berichte aufrufen.

> ➢ Sie erreichen den Berichtbereich, indem Sie auf die Registerkarte ***Berichte*** am linken Bildrand klicken.

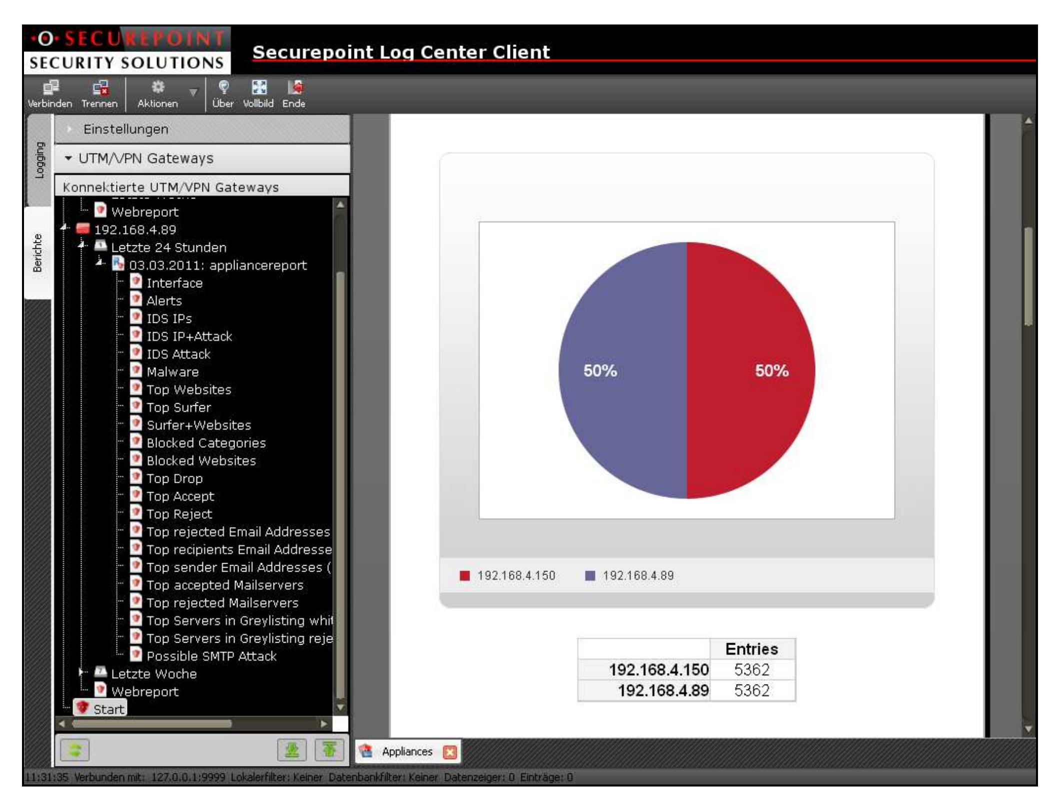


Abb. 125 Berichte Ansicht

> ➢ Wenn Sie mit der ***rechten Maustaste*** auf einen geöffneten Bericht klicken, können Sie aus dem ***Kontextmenü*** weitere Optionen wählen.
>
> - ***Drucken***: Öffnet die Druckvorschau.
> - ***Speichern***: Öffnet den Speicherdialog.
> - ***Zoom***: Öffnet ein Untermenü mit den Optionen ***Zoom in*** (vergrößern), ***Zoom out*** (verkleinern) und ***Zurücksetzen*** auf Normalansicht.



Abb. 126 Kontextmenü der Berichtansicht

13.4 Bericht Einstellungen

Im Menü ***Einstellungen*** können Sie Einstellungen für die Darstellung, Druckoption und Speicherort einstellen.

Bezeichnung	Beschreibung
Hintergrund-bilder drucken	Hintergründe von Grafiken und Tabellenköpfe können für den Druck deaktiviert werden.
Berichts-verzeichnis	In dieses Verzeichnis werden alle Berichte als Zip-Archiv gespeichert, sobald ein Bericht geöffnet wird.
Seitenränder	Hier können Sie die Seitenränder für alle Berichte ändern. Sie können zwischen den Einheiten Millimeter und Punkte (px) wählen
Diagrammtyp in Start	Im Übersichtsbericht für alle Appliances, der über den Eintrag Start abgerufen wird, wird die Verteilung der Logeinträge grafisch dargestellt. Wählen Sie hier zwischen Tortendiagramm und Balkendiagramm.
Doppelklick auf Appliance-Bericht öffnet	Ein Doppelklick auf einen Bericht zeigt den Bericht für verschiedene Zeitspannen. Wählen Sie zwischen letzte 24 Stunden, letzte Woche und letzten Monat.
Doppelklick auf Appliance-Bericht öffnet Tab	Berichte werden in Tabs geöffnet, die am unteren Bildrand eingeblendet werden. Neuen: Berichte werden immer im ersten Tab geöffnet. Der bestehende Tab wird überschrieben. Ersten: Ein neuer Tab wird vor der Tabliste geöffnet. Aktiv: Berichte werden immer im gerade aktiven Tab geöffnet. Ersetzt den aktiven Tab.



Abb. 127 Einstellungen für Berichte

13.5 Berichtliste

Unter dem Menü ***UTM/VPN Gateways*** finden Sie eine Liste ***konnektierte UTM/VPN Gateways***, also Appliances, deren Protokolldaten von diesem Log Center aufgenommen und aufbereitet werden.

In dieser Baumstruktur finden Sie unter jedem Gateway Berichte der letzten 24 Stunden, der letzten Woche und des letzten Monats. Unter diesen wiederum befinden sich Ordner, die die einzelnen Berichte beinhalten. Jeder Ordner ist mit dem jeweiligen Erstellungsdatum benannt.

Die folgende Übersicht erklärt kurz die verfügbaren Berichte.

Bezeichnung	**Beschreibung**
Interface	Zeigt Diagramme über die Interface Auslastung aufgetragen gegen die Zeit. Die Auslastung wird für jedes Interface einzeln ausgegeben. Außerdem werden noch der gesamte Traffic, der gesendete Traffic (TX) und der empfangene Traffic (RX) pro Interface angegeben.
Alerts	Zeigt eine Tabelle über ausgelöste Alarme. Es wird die Anzahl der ausgelösten Alarme und deren Quell IP-Adresse angegeben. Die Auflistung erfolgt außerdem prozentual.
IDS IPs	Listet die IP-Adressen auf, von denen das Intrusion Detection System Angriffe festgestellt hat.
IDS IP+Attack	Listet die IP-Adressen der Angreifer und Angriffsarten auf.
IDS Attack	Tabelle der erkannten Angriffe in absteigender Sortierung des Auftretens.
Malware	Listet entdeckte Malware mit Namen, Art und Anzahl der Vorkommnisse auf.
Top Websites	Listet die Websites auf, die am meisten Traffic verursacht haben. Die Anzahl der Aufrufe ist dabei nicht entscheidend.
Top Surfer	Liste die Nutzer auf, die am meisten Traffic verursacht haben. Die Nutzer werden aufgelistet mit IP-Adresse und AD Nutzername. Beachten Sie bei der Auswertung die Datenschutzbestimmungen Ihres Landes.
Surfer+Websites	Zeigt die meist aufgerufenen Websites in Verbindung mit dem meistaufrufenden Benutzer.
Blocked Categories	Listet die Webseiten-Kategorien auf, die am meisten geblockt wurden.
Blocked Websites	Listet die geblockten Webseiten auf in absteigender Sortierung des Auftretens.

Bezeichnung	Beschreibung
Top Drop	Zeigt ein Diagramm und eine Tabelle mit den meisten fallengelassenen Paketen und deren Quell IP-Adressen.
Top Accept	Zeigt ein Diagramm und eine Tabelle mit den meisten angenommenen Paketen und deren Quell IP-Adressen.
Top Reject	Zeigt ein Diagramm und eine Tabelle mit den meisten zurückgewiesenen Paketen und deren Quell IP-Adressen.
Top rejected Email Addresses with User unkown	Zeigt eine Tabelle mit zurückgewiesenen E-Mails an unbekannte Empfänger.
Top recipients Email Addresses (accepted)	Zeigt eine Tabelle angenommener E-Mails in Beziehung zum Empfänger.
Top sender Email Addresses (accepted and rejected)	Zeigt eine Tabelle der meist angenommenen und abgewiesenen E-Mails in Beziehung zum Absender.
Top accepted Mailservers	Zeigt eine Liste der Mailserver, von denen die meisten angenommenen E-Mails stammen.
Top rejected Mailservers	Zeigt eine Liste der Mailserver, von denen die meisten abgewiesenen E-Mails stammen.
Top Server in Greylisting whitelisted	Zeigt eine Liste der Server, die im Greylisting auf der Whitelist stehen.
Top Server in Greylisting rejected	Zeigt eine Liste der Server, von denen E-Mails durch das Greylisting zurückgewiesen wurden.
Possible SMTP Attack	Zeigt die Server von denen möglicherweise ein SMTP Angriff gestartet worden ist.

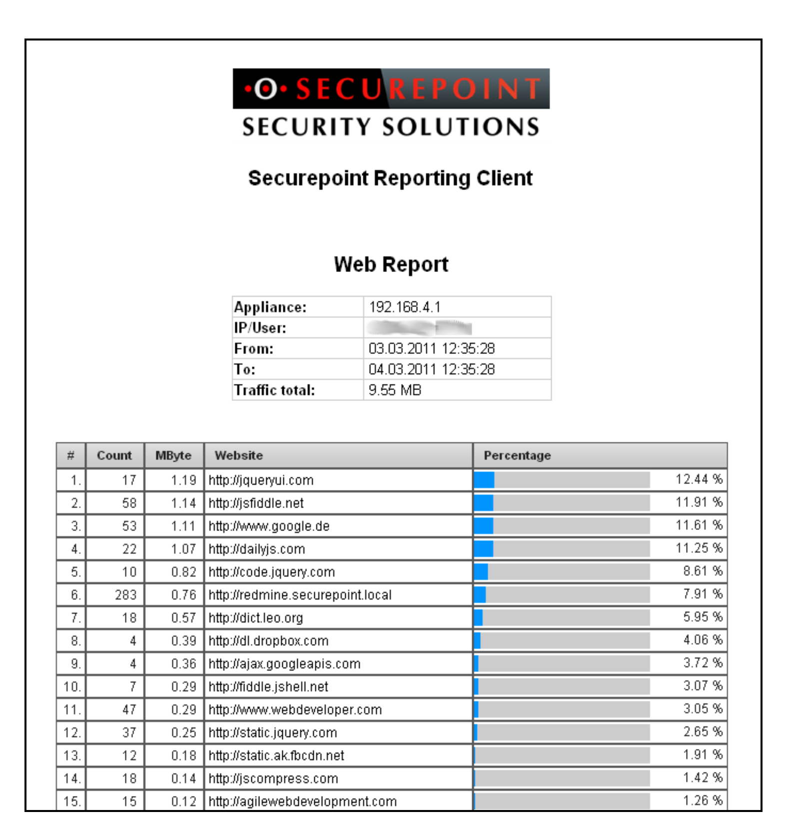
13.6 Webreport

Der Webreport ist ein Bericht für einen bestimmten Benutzer oder für eine bestimmte IP-Adresse. Dieser Bericht wird immer aktuell erstellt. Es wird der gesamte Traffic des Benutzers in dem gewählten Zeitraum angezeigt. In einer Tabelle wird die prozentuale Aufteilung des Datenaufkommens auf die aufgerufenen URLs angezeigt. Für jede gelistete Internetseite werden die Anzahl der Aufrufe und der Traffic angezeigt.

- Klicken Sie im Logclient auf den Reiter ***Berichte*** am linken Fensterrand.
- Öffnen Sie im Menü ***UTM/VPN Gateways*** den Ordnerbaum des Gateways, von der Sie einen Webreport erstellen möchten.
  Der Eintrag Webreport befindet sich in der ersten Ebene.

Abb. 128 Daten für einen Webreport definieren

- Führen Sie auf diesen Eintrag einen ***Doppelklick*** aus oder benutzen Sie das ***Kontextmenü*** und klicken Sie auf ***Ansehen***.
- Geben Sie im erscheinenden Dialog im ***Feld IP/Benutzer*** die IP-Adresse oder den Benutzernamen des Benutzers ein, für den ein Bericht erstellt werden soll.
- Geben Sie im den Feldern ***Startdatum*** und ***Enddatum*** den Zeitraum an, für den ein Bericht angefertigt werden soll. Voreinstellung: letzte 24 Stunden
- Klicken Sie auf ***Ansicht***. Im rechten Fenster wird der Webreport geöffnet.
- Mit einem ***Rechtsklick*** auf den Bericht gelangen Sie zu Druck- und Speicheroptionen.



Securepoint Reporting Client

Web Report

Appliance:	192.168.4.1
IP/User:	[illegible]
From:	03.03.2011 12:35:28
To:	04.03.2011 12:35:28
Traffic total:	9.55 MB

#	Count	MByte	Website	Percentage
1.	17	1.19	http://jqueryui.com	12.44 %
2.	58	1.14	http://jsfiddle.net	11.91 %
3.	53	1.11	http://www.google.de	11.61 %
4.	22	1.07	http://dailyjs.com	11.25 %
5.	10	0.82	http://code.jquery.com	8.61 %
6.	283	0.76	http://redmine.securepoint.local	7.91 %
7.	18	0.57	http://dict.leo.org	5.95 %
8.	4	0.39	http://dl.dropbox.com	4.06 %
9.	4	0.36	http://ajax.googleapis.com	3.72 %
10.	7	0.29	http://fiddle.jshell.net	3.07 %
11.	47	0.29	http://www.webdeveloper.com	3.05 %
12.	37	0.25	http://static.jquery.com	2.65 %
13.	12	0.18	http://static.ak.fbcdn.net	1.91 %
14.	18	0.14	http://jscompress.com	1.42 %
15.	15	0.12	http://agilewebdevelopment.com	1.26 %

Abb. 129 Beispiel für ein Webreport

14 Hotkeys

Einige wichtige Funktionen sind auf den Funktionstasten abgelegt, um diese schnell ausführen zu können. Diese Tasten werden auch Hotkeys oder Short Cuts genannt.

Taste	Funktion
F2	Ordnerbaum im Menü UTM/VPN Gateways aufklappen.
F4	Verbindung zu einem Gateway beenden.
F5	Vom SOC abmelden. Beendet das SOC nicht. Funktioniert nur, wenn keine Gateway-Verbindung aktiv ist.
F11	Schaltet in den Vollbildmodus und zurück.
F12	Macht einen Screenshot mit anschließendem Speicherdialog.